ESCUELA POLITÉCNICA NACIONAL

FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA

DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN, BASADO EN LA NORMA ISO/IEC 27001:2013, PARA UNA FÁBRICA DE CUERO Y CALZADO

TRABAJO DE TITULACIÓN PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERA EN ELECTRÓNICA Y REDES DE INFORMACIÓN

VICTORIA ELIZABETH CAMACHO MUNCHA

DIRECTOR: MSc. PABLO WILIAN HIDALGO LASCANO

Quito, Noviembre 2021

AVAL

Certifico que el presente trabajo fue desarrollado por la señorita Victoria Elizabeth Camacho Muncha, bajo mi supervisión.

MSc. PABLO HIDALGO
DIRECTOR DEL TRABAJO DE TITULACIÓN

DECLARACIÓN DE AUTORÍA

Yo, Victoria Elizabeth Camacho Muncha, declaro bajo juramento que el trabajo aquí descrito es de mi autoría; que no ha sido previamente presentado para ningún grado o calificación profesional; y, que he consultado las referencias bibliográficas que se incluyen en este documento.

A través de la presente declaración dejo constancia de que la Escuela Politécnica Nacional podrá hacer uso del presente trabajo según los términos estipulados en la Ley, Reglamentos y Normas vigentes.

Victoria Elizabeth Camacho Muncha

DEDICATORIA

A Dios, por estar presente en mi mente y corazón todos los días de mi vida; y permitirme despertar cada día para disfrutar del amor de mi familia y del pan de cada día.

A usted mamita que siempre aplaudió mis logros, estuvo en los momentos que más la necesité y porque gracias a usted soy una mujer humilde, sencilla y valiente. Hoy cumplo lo que le prometí en aquella cama de UCI y sé que estará orgullosa de mí. Gracias por la vida mamita.

A usted papito por ser el hombre de mi vida, un ejemplo de lucha, fe, valores y principios que me definen quien soy ahora. Por ser un buen padre, amigo y consejero quién confió y me apoyó en todas las decisiones que he tomado en mi vida.

A mis hermanos Milton, Norma, Rubén, Diana y Carmita por ser mi espejo en todo momento, porque gracias a ustedes he podido conocer el amor de hermanos, el afecto y cariño sincero; y el soporte que han sido para no dejarme caer.

A mis cuñadas/os Mónica, Jason, Laura y Marlon porque día a día fueron luz en mi camino y han confiado en mí una hermana más.

A mis sobrinos Bryan, Alexis, Valentina, Alejandrina y Catalina porque gracias a sus ocurrencias me han sacado una sonrisa en medio de lágrimas de tristeza.

A todos mis tíos y primos que estuvieron presentes en el camino de la vida.

Vicky

AGRADECIMIENTO

Agradezco a Dios por ser un pilar fundamental en mi vida, por ser mi luz y fortaleza en los caminos de obscuridad y por regalarme un día más de vida.

Quiero dar gracias una vez más a mis padres Elías Camacho y Carmen Muncha (+), a mis hermanos/as, a mis cuñadas/os y a mis sobrinos quienes estuvieron presentes en todo momento, fueron mi guía para alcanzar esta meta gracias a su paciencia, perseverancia y confianza sigo aquí firme.

Gracias a ti, Johis porque fuiste un gran apoyo cuando estaba triste y quería desistir de todo, siempre estuviste ahí. Gracias por ser mi amiga incondicional, por poner mi vida en perspectivas diferentes y apoyarme en todas mis decisiones.

Gracias a ustedes Alexander, Mary y Katyliz por los años de amistad compartidos, por ser mi apoyo incondicional, por sostenerme y regalarme muchas alegrías.

Quiero expresar mi gratitud a usted Ing. Pablo Hidalgo por ser mi tutor de tesis, por la paciencia y el compromiso que tuvo conmigo este tiempo. Por los conocimientos impartidos en las aulas, consejos, anécdotas y sabiduría para culminar este proyecto.

Quiero agradecer a Wilmita Guerrero quien fue mi ángel de luz en mi carrera universitaria, una gran mujer que confió en mí y con sus abrazos me daba paz.

Gracias a ustedes Gaby, Rita, Marco, Leo, Santi y Juancho por estar ahí pendientes de mí, por reír y llorar conmigo en los momentos de triunfos y fracasos.

A ustedes Sami, Ale, Julio, Harry, Andre, Juank, Cris, Oscar, Javi, Jorge, Eddy, Chris I. y Paúl, que con ustedes compartí momentos bonitos en las aulas y fuera de ellas. A ustedes Jona, Giovi, Dani, Pame, Darwin, Xavi, Alejita, Carlitos, Karlita y Fer porque fueron una segunda familia. A ustedes Karlita, Sarita, Gis, Fabi, Alex A., David, Andrés, Kari y Darwin que junto a ustedes emprendí este camino. A ustedes Fabri, Pavo, Andrés, Paúl, Alex, Erick, Dino, Joss y Ramiro porque sin ustedes me hubiese graduado antes.

A ustedes Kathy L., Carlita S., Javo, Pancho, Mayrita T., Anita, Sandrita L., Henry C. y Danny B. quienes con su forma de ser me regalaron alegría en el camino.

Vicky

ÍNDICE DE CONTENIDO

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

RESUMEN

La empresa de cuero y calzado Curtiembre Quisapincha busca crecer en el mercado digital, brindar confidencialidad y transparencia de datos a todos sus clientes y proveedores. Con este propósito se desarrolla el presente Trabajo de Titulación que tiene como objetivo diseñar un SGSI (Sistema de Gestión de Seguridad de la Información), que consta de 4 capítulos y 9 Anexos.

El primer capítulo abarca la introducción, objetivos y alcance del proyecto; recopila el fundamento teórico y herramientas de las normas ISO/IEC 27000 así como la metodología MAGERIT v.3.

El segundo capítulo expone la metodología de este proyecto, misma que está compuesta de tres cláusulas que son parte de la norma ISO/IEC 27001:2013; la primera referida al Contexto de la Organización, la segunda cláusula relacionada al Liderazgo que establece el compromiso de la Alta Dirección de la empresa con el SGSI y la tercera cláusula que define la Planificación, cuyo enfoque permite determinar los criterios de valoración y establecimiento de una metodología para el SGSI, esta última basada en MAGERIT v.3 e ISO/IEC27001:2013.

El tercer capítulo presenta el análisis de resultados y las políticas de seguridad de la información elaboradas para la empresa, las cuales son definidas para la implementación del SGSI.

El cuarto capítulo comprende de las conclusiones basadas en el desarrollo y resultados obtenidos, así también las recomendaciones pertinentes al desarrollo e implementación del SGSI.

Como resultado del desarrollo del proyecto se obtuvieron un total de 36 activos de información, así también se identificaron 395 riesgos asociados a los activos de la empresa y para contrarrestar dichos riesgos de seguridad de la información se seleccionaron 64 controles que permitirán reducir el riesgo a futuro.

Los Anexos contienen las tablas y matrices obtenidas del análisis y gestión de riesgos, así como el tratamiento de los riesgos; también incluye la entrevista al Jefe del Área de Tecnologías de la Información de la empresa.

PALABRAS CLAVE: ISO/IEC 27000, ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27005, MAGERIT, SGSI, Sistema de Gestión de la Seguridad de la Información

ABSTRACT

The leather and footwear company Curtiembre Quisapincha seeks to grow in the digital market, providing confidentiality and data transparency to all its customers and suppliers. With this purpose in mind, this degree work is developed, which aims to design an ISMS (Information Security Management System). This Degree Project is made up of 4 chapters and 9 Annexes.

The first chapter covers the introduction, objectives and scope of the project; compiles the theoretical foundation and tools of the ISO / IEC 27000, 27001, 27002 and 27005 standards, as well as the MAGERIT v.3 methodology.

The second chapter exposes the methodology of this project, which is composed of three clauses as indicated in the ISO / IEC 27001: 2013 standard. The context of the organization is the first clause, the second clause is the Leadership that establishes the commitment of the Senior Management of the company with the ISMS, and the third clause is Planning, which approach allows determining the evaluation criteria and establishment of a methodology for the ISMS, the latter based on MAGERIT v.3 and ISO / IEC27001: 2013.

The third chapter contains the analysis of the results and the information security policies developed for the company, which are defined for the implementation of the ISMS.

The fourth chapter includes the conclusions based on the development and results obtained, as well as the pertinent recommendations for the development and implementation of the ISMS.

As a result of the development of the project, a total of 36 information assets were obtained, as well as 395 risks associated with the company's assets and to counteract these information security risks, 64 controls were selected that will reduce the risk in the future.

The Annexes contain the tables and matrices obtained from the risk analysis and management, as well as the treatment of risks; The interview with the Head of the Information Technology Area is also included, which allows to determine the current situation of the company.

KEYWORDS: ISO / IEC 27000, ISO / IEC 27001, ISO / IEC 27002, ISO / IEC 27005, MAGERIT, ISMS, Information Security Management System

1. INTRODUCCIÓN

En la actualidad, la rápida digitalización del entorno comercial de los consumidores e industrias debido a la pandemia del COVID-19, ha ejercido una enorme presión en su entorno digital que no estaba preparado para un cambio total e inesperado. Debido a este cambio y a la falta de concientización en ciberseguridad, se han generado brechas de seguridad fáciles de vulnerar; por ejemplo, el uso de varias plataformas digitales como medios de videoconferencia, conexión remota, medios y redes sociales, aplicaciones web y móviles son los principales blancos para un ataque de ciberseguridad.

Según una investigación a nivel mundial realizada por RiskIQ [1], en 2018, el costo por minuto de un ciber-delito fue de $1,2 millones a razón de ataques como *rasomware*[1], *malware*[2] y *phishing*[3]. En 2019, el costo por minuto fue de 2,9 millones debido a "hackeos" en *crypto-moneda, phishing, rasomware* y ataques de Magecart[4]. En 2020, la cifra se incrementó exponencialmente a $11,4 millones por minuto como se observa en la Figura 1.1, debido a vulnerabilidades reveladas, *phishing*, aplicaciones móviles, correos spam, nuevos host y dominios infectados referentes al COVID-19.

Figura 1.1. Costo de ciber-delito por minuto

En Ecuador, varias industrias y empresas se vieron forzadas a la adopción tecnológica en el comercio, por lo tanto, se reinventaron a través del comercio electrónico, transacciones

[1] *Rasomware*: *Software* malicioso que infecta los dispositivos electrónicos y exige el pago de dinero para poder acceder a ellos.
[2] *Malware*: *Software* o código malicioso que invade el funcionamiento normal de un dispositivo.
[3] *Phishing*: Técnica de ciberataque que consiste en engañar a una víctima para obtener datos privados de los usuarios, cuentas y datos bancarios a través de internet.
[4] Magecart: Grupo de *hackers* que roba datos de tarjetas de pago, a través de un *web skimmer*, quien monitoriza continuamente los eventos de un sitio web.

digitales y ventas a través de redes sociales, para sobresalir con sus negocios. Este comercio digital tuvo un incremento inesperado del 3% al 95%, niveles que reflejan un impulso acelerado en el país, debido a las restricciones establecidas durante la pandemia vivida a nivel mundial [2]. Como consecuencia, toda la información manejada a través de medios digitales se encuentra vulnerable y susceptible a ataques de ciberseguridad, que pueden generar altos costos por pérdida de datos [3]. Esto implica que se debería diseñar e implementar un SGSI (Sistema de Gestión de la Seguridad de la Información), para proteger los activos de información y mejorar continuamente el entorno de seguridad de la información [4].

De acuerdo con lo antes mencionado, negocios como fábricas de cuero y calzado no cuentan con la certificación ISO-IEC 27001:2013 [5], la misma que permite garantizar el buen manejo de la seguridad de la información. Las estadísticas proporcionadas en la encuesta sobre las certificaciones válidas a nivel mundial en 2018 indican que Ecuador tiene únicamente ocho certificaciones reportadas por las entidades certificadoras de la ISO-IEC 27001:2013 [6], las cuales corresponden a Tecnologías de la Información (TI) como se indica en la **Figura 1.2**.

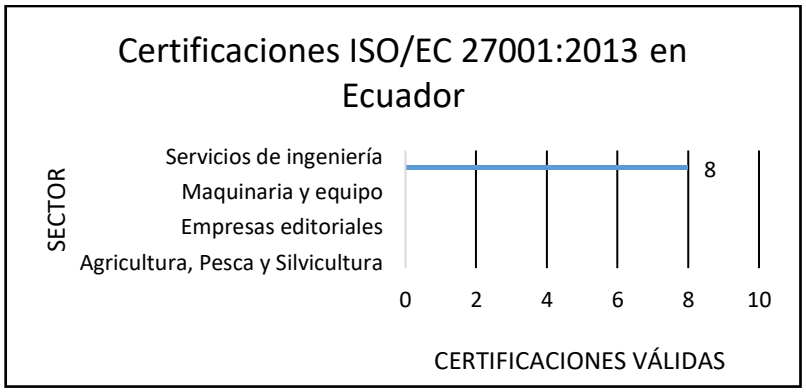


Figura 1.2. Certificaciones válidas ISO-IEC 27001:2013 en Ecuador *[6]*

En la provincia de Tungurahua, varias fábricas de cuero han venido manejando los procesos y la gestión de la información de una forma empírica. Por ejemplo, fábricas de calzado como Plasticaucho Industrial S.A. realizan el manejo interno de políticas de seguridad de la información de forma escasa [7], es decir que no cuentan con un SGSI avalado por una entidad certificadora de la ISO (Organismo Internacional de Normalización) / IEC (Comisión Electrotécnica Internacional). Por lo tanto, la información de la empresa se encuentra expuesta a riesgos y ataques, que en el caso de materializarse podrían generar pérdidas económicas.

Conforme a todo lo mencionado, se propone diseñar un SGSI en base a las necesidades y requerimientos de una fábrica de cuero y calzado, ubicada en la parroquia Quisapincha del cantón Ambato. El diseño podrá ser implementado posteriormente y permitirá un mejor manejo de la información; su implementación permitirá minimizar los riesgos e impactos en caso de existir alguna incidencia de seguridad y proveerá una solución basada en controles de seguridad, que disminuirá el riesgo calculado en base a un análisis de gestión de riesgos de los activos de dicha fábrica.

Si no se realiza el presente proyecto, no se dispondrá de un SGSI diseñado con los requerimientos de una fábrica de cuero y calzado y como resultado se seguirá manejando la seguridad de la información de forma empírica, sin ningún tipo de procedimiento establecido.

1.1. OBJETIVOS

El objetivo general de este trabajo de titulación es Diseñar un Sistema de Gestión de la Seguridad de la Información, basado en la norma ISO/IEC 27001:2013, para una fábrica de cuero y calzado.

Los objetivos específicos son:

- Revisar la información y normas ISO/EC 27001:2013 relacionadas con el fundamento teórico necesario para el desarrollo del proyecto.
- Analizar el sistema de información existente de la empresa, asociado a los riesgos de la seguridad de la información.
- Gestionar los riesgos de la seguridad de la información en base a la metodología MAGERIT (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información).
- Definir controles de seguridad de la información en base a la gestión de riesgos de la empresa y al Anexo A de la norma ISO/EC 27001:2013.

1.2. ALCANCE

El presente trabajo de titulación propone el diseño de un SGSI en base a la información de la fábrica de cuero y calzado “Curtiembre Quisapincha”; dicho diseño es un conjunto de procedimientos, controles y políticas que tiene como objetivo la búsqueda de la protección de los activos de información y la mejora continua del entorno de seguridad de la empresa.

El diseño se realizará para la infraestructura tecnológica e información de la empresa, no se tomará en cuenta el activo recurso humano e infraestructura física no tecnológica.

Para diseñar el SGSI se realizará un estudio de las normas NTE[5] INEN[6] ISO/IEC 27000:2016, NTE INEN- ISO/IEC 27001:2013, NTE INEN- ISO/IEC 27002:2013 y NTE INEN- ISO/IEC 27005:2012. En la norma NTE INEN- ISO/IEC 27001:2013 se establece dentro de la cláusula 6.1.2 que se debe definir la metodología de gestión (análisis y evaluación) de riesgos, por lo que se ha considerado la metodología MAGERIT, para realizar dicha gestión.

Para empezar con el desarrollo del diseño se realizará un análisis de la empresa; para esto se recolectará toda la información (documentación, datos y entrevistas) necesaria que la empresa posea con el fin de detectar los riesgos y amenazas que no están técnicamente tratados, y así determinar un listado actual de los requerimientos y necesidades que se consideren necesarios para la empresa.

Dentro de este análisis, adicionalmente se identificarán los controles (salvaguardas) existentes en la empresa, para posteriormente valorar la eficiencia de éstos, en base al análisis de riesgos realizado.

Toda la información de la situación actual de la empresa, así como la de sus requerimientos y controles existentes se determinarán en base a entrevistas al jefe del Área de Tecnologías de la Información y al gerente de la empresa.

Una vez obtenidos los requerimientos de la empresa se procederá a realizar la gestión de riesgos con la metodología MAGERIT, metodología que implica la valoración de activos, la identificación de amenazas y evaluación de riesgos. El tratamiento de los riesgos y selección de controles se lo realizará en base al Anexo A de la norma NTE INEN- ISO/IEC 27001:2013.

Para la valoración de activos, se debe partir de un inventario que se obtendrá a través de entrevistas con el personal encargado del área de Sistemas y de los requerimientos de la empresa. El objetivo de realizar esta valoración es obtener un inventario de todos los activos en función de su valor propio.

La valoración de cada activo se la realizará de forma cuantitativa en base a las dimensiones de seguridad de la información (Integridad, Confidencialidad y Disponibilidad); esta valoración se realizará de acuerdo con el nivel de afectación en el caso de existir un fallo en el activo. Se incluirá también la valoración cualitativa del costo de cada activo.

[5] NTE: Norma Técnica Ecuatoriana
[6] INEN: Servicio Ecuatoriano de Normalización

Se realizará la identificación de amenazas para cada activo, tomando en cuenta la degradación del valor del activo, la probabilidad de ocurrencia de dicha amenaza y el impacto que provoca.

Antes de efectuar el tratamiento de los riesgos, es decir definir los controles que constan en el Anexo A de la ISO-IEC 27001:2013, necesarios para disminuir el Riesgo Actual que tiene la empresa, se realizará un documento de aplicabilidad en donde se definirán cuáles controles se establecerán y cuáles no, con su debida justificación en base al giro del negocio. En el tratamiento de riesgos se establecerán los controles (salvaguardas) con el fin de disminuir el Riesgo Potencial. Con esto se obtendrá el Riesgo Actual y el Riesgo Planificado.

Se entregará un resumen ejecutivo de los resultados obtenidos, en donde se detallará el análisis que se llevó a cabo de los riesgos encontrados y los controles que se basaron en el documento de aplicabilidad necesarios para disminuir ese riesgo. Además, se presentará un documento que detalle un conjunto de políticas y procedimientos dentro del SGSI basado en el Anexo A de la ISO 27001:2013 para la seguridad de la información de la empresa.

Los análisis y cálculos se mostrarán en una matriz de gestión de riesgos.

Se establecerán conclusiones y recomendaciones, las cuales podrían ser útiles para trabajos futuros relacionados a este modelo de empresa.

El presente trabajo de titulación no presentará un producto final demostrable.

1.3. MARCO TEÓRICO

A continuación, se expondrá de forma breve conceptos teóricos fundamentales para el desarrollo del Sistema de Gestión de Seguridad de la Información propuesto.

1.3.1. FUNDAMENTOS DE SEGURIDAD DE LA INFORMACIÓN

1.3.1.1. INFORMACIÓN

La información es un conjunto de datos procesados que constituyen un activo valioso de una organización y requiere una protección adecuada [8]. Estos datos pueden estar en formato digital (en los dispositivos electrónicos y ópticos), físico (en papel) e intangible (en conocimiento y experiencia), y puede ser transmitida a través de medios electrónicos, mensajería o verbal, respectivamente. Considerando lo mencionado, la tecnología es un elemento indispensable en una organización y ayuda a facilitar la creación, procesamiento, almacenamiento, transmisión, protección y destrucción de la información [9].

1.3.1.2. ACTIVO

Un activo es cualquier elemento que tenga valor para una organización. La importancia de un activo se incrementa según la criticidad de la información contenida y según el tipo de afectación que podría tener si ocurre un incidente de seguridad [9].

1.3.1.3. AMENAZA

Una amenaza es la causa potencial de un incidente de seguridad, que al materializarse puede ocasionar perjuicios al funcionamiento de una organización [10].

1.3.1.4. RIESGO

El riesgo es la estimación de la probabilidad de que una amenaza se materialice sobre los activos, causando graves daños y pérdidas a la organización, así también afectando a la imagen y misión de esta [11].

1.3.1.5. INCIDENTE DE SEGURIDAD

Un incidente de seguridad es un evento inesperado que se produce por la materialización de una o más amenazas sobre un activo, lo que produce un daño o alteración a las operaciones, procesos y activos de una entidad [12].

Algunos ejemplos de incidentes de seguridad son: fraude, *phishing*, alteración de datos, divulgación no autorizada de información personal, ataque por inserción de código malicioso, denegación de servicio (DoS, *Denial of Service*) [13].

1.3.2. SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Un SGSI es un conjunto de políticas, procesos, directrices y recursos gestionados de manera colectiva por una organización. El objetivo principal de un SGSI es la búsqueda de la seguridad de la información mediante la protección de los activos en base al análisis de riesgos y la mejora continua de los procesos para alcanzar los objetivos de negocio de una organización pública o privada [14].

El diseño e implementación de un SGSI requiere del apoyo de toda la organización, debido a que todo el sistema estará en función de las necesidades y requerimientos de esta, por lo tanto, se necesita ayuda de la alta dirección, personal, accionistas, proveedores de servicios externos y otras partes interesadas. Esto debido a que existen una serie de procesos y controles para cada activo de la organización y se requiere de la concientización del factor humano, en función de la seguridad de la información [14].

1.3.2.1. Beneficios de un SGSI

Existen varios beneficios de los SGSI aplicados a cualquier tipo de organización y actividad comercial, incluidas las PYMES (Pequeñas y Medianas Empresas). Es esencial que controlen y gestionen la seguridad de la información y *ciber-riesgos* para protegerse y brindar seguridad a su cadena de suministro [15]**.**

Como se muestra en la **Figura 1.3** existen varias características que benefician tanto a grandes empresas y PYMES, como también al sector privado. A continuación, se listan los beneficios que brinda:

- Ayuda a mejorar la evaluación de riesgos.
- Proporciona buenas prácticas de seguridad de TI.
- Mejora la defensa frente a ciberataques.
- Refuerza la seguridad de la información.
- Mantiene la confidencialidad.
- Aumenta la integridad personal.
- Combate los riesgos relacionados con dispositivos móviles.
- Demuestra buenas prácticas de seguridad.
- Infunde confianza al cliente.
- Va en línea con otras normas de sistemas de gestión.
- Previene el robo de identidad.

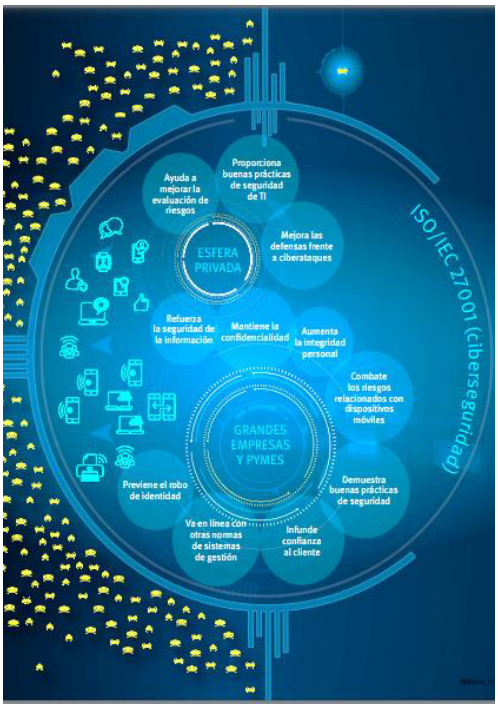


Figura 1.3. ISO/IEC 27001 (Ciberseguridad) *[15]*

1.3.3. FAMILIA DE NORMAS DEL SGSI

Los Sistemas de Gestión de la Seguridad de la Información son sistemas basado en la familia de normas ISO27001, que es un conjunto de buenas prácticas para el establecimiento, implementación, mantenimiento y mejora de, que se encuentran expresadas a través de estándares internacionales relacionados con la Seguridad de la Información [12].

Esta familia de normas se encuentra relacionada de una forma estrecha y su clasificación se muestra en la **Figura 1.4**.

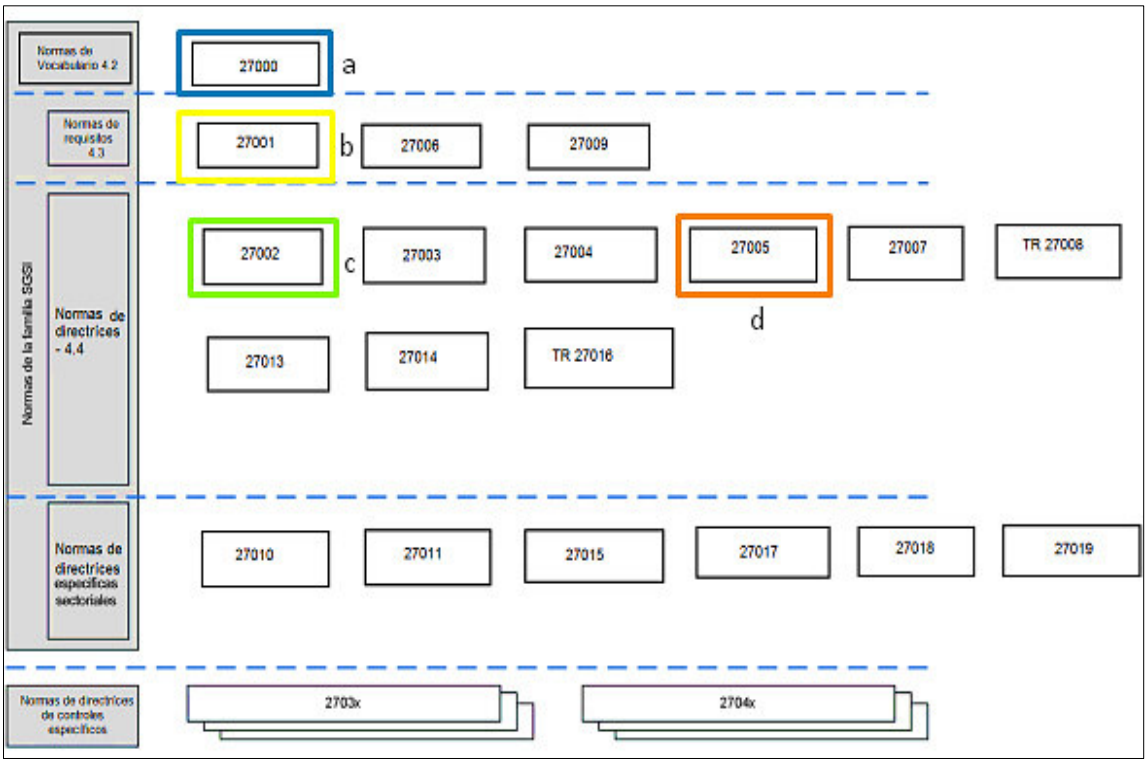


Figura 1.4. Relación entre normas de la familia SGSI *[12]*

En la Figura 1.4 en el literal *a*, se tiene un grupo de normas de vocabulario que hace referencia a la ISO/IEC 27000 que especifica una visión general de las normas y el vocabulario de un Sistemas de Gestión de Seguridad de la Información [10].

Se indican también las normas de requisitos de las cuales únicamente la ISO/IEC 27001 que refiere a los requisitos de un Sistemas de Gestión de Seguridad de la Información, tal como se señala en el literal *b* de la Figura 1.4 [10].

Las normas de directrices brindan reglamentos generales, así como la orientación para la implementación de controles. Las normas que serán de gran utilidad en el presente

proyecto es la norma ISO/IEC 27002 que refiere al código de conducta para controles de seguridad de la información y la norma ISO/IEC 27005 que especifica la gestión de riesgos de seguridad de la información, tal como se señala en la Figura 1.4 en los literales *c* y *d,* respectivamente [10].

Las normas de directrices especificas sectoriales tienen un enfoque relacionado a la seguridad de la información de empresas con roles específicos como telecomunicaciones, servicios financieros, servicios en la nube, servicios de energía, etc [10].

Las normas de directrices de controles específicos hacen referencia a la seguridad de la red, aplicaciones, gestión de incidentes y directrices para distintas áreas tecnológicas del futuro [10].

A continuación, se mencionan las normas que serán utilizadas como fuente de información para la elaboración del presente proyecto.

1.3.3.1. Norma Técnica Ecuatoriana INEN-ISO/IEC 27000:2016

Esta norma brinda información introductoria sobre los Sistemas de Gestión de Seguridad de la Información, campos de aplicación, importancia y beneficios de la familia de normas del SGSI. Además, sintetiza un breve contenido de vocabulario y definiciones referentes a los Sistemas de Gestión de Seguridad de la Información, así también explica de manera simplificada el contenido de cada norma correspondiente a la familia de normas del SGSI [12].

1.3.3.2. Norma Técnica Ecuatoriana INEN-ISO/EC 27001:2013

La ISO/IEC 27001 describe las “Tecnologías de la Información – Técnicas de Seguridad – Sistemas de Gestión de Seguridad de la Información – Requisitos (ISO/IEC 27001:2013+Cor.1.2014+Cor.2_2015.)”, esta norma específica los requisitos para el diseño e implementación de un Sistema de Gestión de Seguridad de la Información, basado en las necesidades y requerimientos de una organización. Esta norma puede ser aplicada a cualquier empresa, independientemente de su tipo, tamaño y naturaleza [14].

1.3.3.2.1. Estructura de la ISO 27001:2013

En la **Figura 1.5** se indica de forma resumida la estructura de la norma ISO/IEC 27001:2013 y la estructura del Anexo A, que posee un conjunto de dominios, objetivos de control y controles para la mitigación de los riesgos para proteger la información a través de la implementación de un SGSI [14].

Para el cumplimiento y diseño de un SGSI se deben efectuar las cláusulas mandatorias que se indican en la **Figura 1.5** de las cuales el presente proyecto cumplirá con las cláusulas Contexto de la Organización, Liderazgo y Planificación debido a que están enfocadas a la parte del diseño del SGSI, mientras que las cláusulas de Soporte, Operación, Evaluación de Desempeño y Mejora, tienen un enfoque hacia la implementación y el cumplimiento del SGSI; lo cual no es parte del alcance de este trabajo de titulación.

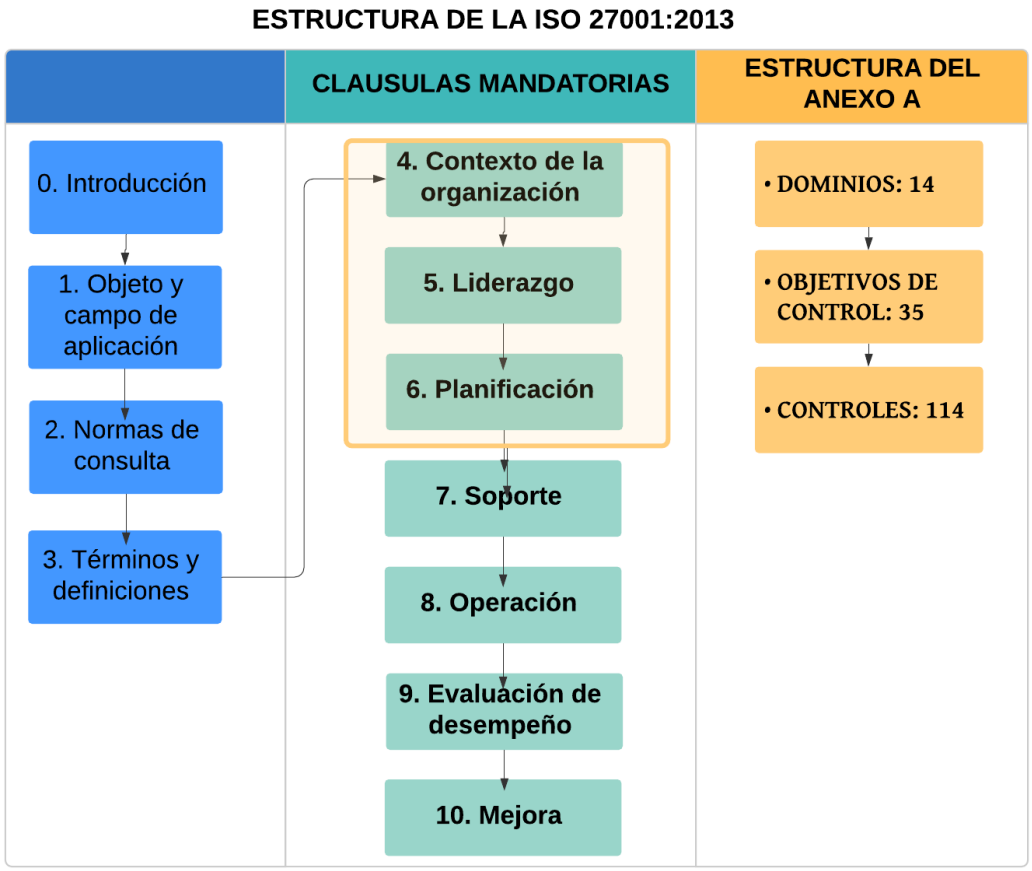


Figura 1.5. Estructura de la Norma ISO/IEC 27001:2013 *[16]*

Las cláusulas a tratarse son las siguientes:

Cláusula N°4: Contexto de la organización

El contexto de la organización se refiere a los factores/cuestiones internas y externas relevantes para el propósito de la organización y en qué medida afectan a la capacidad para el cumplimiento de resultados deseados del SGSI. Se debe determinar el alcance del SGSI, es decir, establecer los límites y la aplicabilidad del SGSI. Además, se debe establecer, implementar, mantener y mejorar continuamente el Sistema de Gestión de Seguridad de la Información [14].

Cláusula N°5: Liderazgo

Esta cláusula hace referencia al liderazgo y compromiso con el que se debe llevar a cabo el SGSI. La alta dirección es parte importante en el desarrollo, pues es quien garantiza que las políticas y objetivos sean compatibles con la estrategia de la empresa; además debe asegurar que los recursos necesarios estén disponibles para obtener los resultados esperados y mantener el compromiso de mejora continua del SGSI. Así también, la alta dirección debe establecer una política de seguridad de la información que cubra los requerimientos de la organización. En el caso de que se implemente el SGSI se deberá delegar a un responsable del área de seguridad de la información, quien tendrá responsabilidades para garantizar el cumplimiento y el desempeño del SGSI [14].

Cláusula N°6: Planificación

La planificación es la etapa en donde se definen y establecen los criterios para hacer estimaciones en el análisis de riesgos de seguridad de la información. Es responsable de determinar los riesgos de seguridad de la información asociados a la pérdida de integridad, confidencialidad y disponibilidad de la información en el alcance del SGSI; también debe identificar a los propietarios de los riesgos [14].

Una vez definidos los criterios se debe analizar los riesgos de la seguridad de la información con el propósito de valorar las potenciales amenazas que se tuviera y el impacto que generaría como resultado, en el caso que los riesgos se materializaran, así también se debe analizar la degradación del valor de cada activo y la probabilidad de ocurrencia real de los riesgos sobre los activos. [14]. En esta etapa se usa una de las metodologías de análisis de gestión de riesgos; en este proyecto se hará uso de la metodología MAGERIT v.3 y la norma ISO 27001:2013.

La Declaración de Aplicabilidad en función del Anexo A de la ISO 27001:2013, es indispensable durante el análisis de gestión de riesgos debido a que en función de esto se seleccionan los objetivos de control y controles aplicables a los activos dentro del giro del negocio. Los mismos deberán ser justificados en el caso de implementarse o no.

Para el tratamiento del riesgo se tienen cuatro opciones: reducción, retención, evitación y transferencia del riesgo, de las cuales se debe seleccionar cómo se va a dar tratamiento a cada riesgo con una de estas opciones y en función de los resultados de estimación del riesgo.

Finalmente, se procede a identificar todos los controles necesarios para implementar las opciones seleccionadas en la etapa de tratamiento de riesgos de seguridad de la

información, dichos controles se deben seleccionar del Anexo A de la ISO 27001:2013 y en función de Documento de Aplicabilidad. Además, se debe indicar un plan de tratamiento de riesgos de seguridad de la información y conseguir su aprobación, así como la admisión de los riesgos de seguridad de la información por parte de los propietarios de estos.

1.3.3.3. Norma Técnica Ecuatoriana INEN-ISO/IEC 27002:2013

Esta norma técnica está diseñada para que las organizaciones la utilicen como referencia durante la selección de controles y en el desarrollo de directrices de un Sistema de Gestión de Seguridad de la Información. También muestra un conjunto de buenas prácticas para la gestión de seguridad de información y objetivos de control [9].

Esta norma junto con la ISO/IEC27001 proporcionan la orientación para la implementación de controles y puesta en marcha de un Sistema de Gestión de la Seguridad de la Información.

1.3.3.4. Norma Técnica Ecuatoriana INEN-ISO/IEC 27005:2012

La ISO/IEC 27005 tiene como enfoque brindar una guía sobre la gestión de riesgos de la seguridad de la información y asesoramiento sobre el análisis completo de la evaluación de riesgos [17].Las normas ISO/IEC27002 y ISO/IEC27005 se las utilizará como objeto de guía de técnicas, procesos y ayuda para complementar el análisis y evaluación de gestión de riesgos.

1.3.4. METODOLOGÍA MAGERIT v.3

Uno de los objetivos del presente trabajo de titulación es conocer, comprender y hacer uso de una Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, la cual se abordará en esta sección.

Para empezar, MAGERIT fue elaborada por el Consejo Superior de Administración Electrónica (CSAE), siendo su última actualización en octubre del 2012. Tiene como objetivo la gestión de los riesgos ocasionados por la dependencia de la sociedad a las tecnologías de la información; es decir, su misión principal es proteger los activos informáticos de una organización en el marco de las Dimensiones de Seguridad [10].

MAGERIT posee algunos objetivos para hacer más sencillo el proceso de análisis de riesgos, de forma que no se dependa de la arbitrariedad del analista, ni se deje lugar a la improvisación; entre ellos se tienen [10]:

1. Hacer que los responsables de las organizaciones de información tomen conciencia de la existencia de los riesgos y la necesidad de gestionarlos.

2. Brindar un método sistemático para el análisis de riesgos que provienen del uso de las Tecnologías de Información y Comunicación (TIC).
3. Apoyar al descubrimiento y planificación del tratamiento más adecuado para conservar bajo control el riesgo.
4. Entrenar a la organización para diferentes circunstancias donde se deba aplicar los procesos de: auditoría, evaluación, certificación y/o acreditación.

La seguridad se define como la capacidad de resistir con cierto grado de nivel de confianza, acciones ilícitas y/o malintencionadas o accidentes que puedan comprometer factores como la Disponibilidad, Autenticidad, Integridad y Confidencialidad de la información almacenada o transmitida; y de los servicios que ofrecen los sistemas informáticos o las redes [10].

En la **Tabla 1.1** se detallan todas las dimensiones de la seguridad consideradas en MAGERIT v.3. En el presente proyecto únicamente se tratarán tres dimensiones que son: Disponibilidad, Integridad y Confidencialidad.

Tabla 1.1. Dimensiones de la seguridad

Dimensión de la seguridad	Descripción
Disponibilidad	También conocida como disposición, es la propiedad que permite acceder a los activos de la organización cada y cuando se requiera. Hay interrupción en el servicio cuando se carece de disponibilidad y, además, afecta a la productividad de la organización, directamente [10].
Integridad	Interfiere directamente con el correcto desempeño de las actividades de una organización. La integridad se refiere a que la información se debe conservar completa y correcta sin ser manipulada, incompleta o corrupta [10].
Confidencialidad	Se refiere al acceso de los datos solo al personal autorizado; es un factor crítico, puesto que puede poner en peligro la credibilidad de la organización, con la suposición del incumplimiento de compromisos contractuales y leyes respectivos a la tenencia de la información [10]. Las principales amenazas son las filtraciones de datos y/o fuga de información, y los accesos no autorizados [10].
Autenticidad	Es la propiedad que verifica la identidad de la entidad o garantiza la fuente de donde proviene la información. En el caso de la información, lo opuesto a la autenticidad pueden ser la manipulación del contenido de los datos o del origen de estos, y para el caso de los usuarios se puede tener una suplantación de identidad en los servicios de acceso [10].
Trazabilidad	Se encarga de asegurar la información para determinar en qué momento y quien ejecutó alguna acción en la organización; es un factor clave para la integridad de los registros. Es fundamental en el análisis de los incidentes, persecución de los atacantes y aprendizaje de la experiencia [10].

1.3.5. MÉTODOLOGÍA DE ANÁLISIS Y GESTIÓN DE RIESGOS

Para el presente proyecto se han establecido varios pasos a seguir para el análisis y gestión de riesgos según MAGERIT [10] y la norma ISO 27001:2013 [14], los que constituyen una metodología en función de los requerimientos de la empresa.

1.3.5.1. Activos

1.3.5.1.1. Identificación de Activos

Para empezar, se debe tener claro dos componentes principales, la información que se utiliza y los servicios que se presta, los cuales ayudan a la identificación de los requerimientos de seguridad para el resto de los elementos del sistema. En la **Tabla 1.2** se pueden observar los activos más importantes [11].

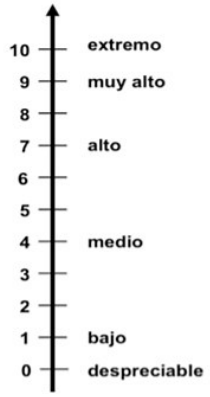
Tabla 1.2. Clasificación de activos *[11]*

Tipo de activo	Descripción
Activos esenciales [Essential]	Es la información o datos que se manejan y los servicios que se prestan, un ejemplo claro de esto son los datos de carácter personal.
Arquitectura del sistema [Arch]	Son los elementos que permiten la estructuración del sistema, con el correcto delineamiento de la arquitectura interna y la relación que guarda con el exterior.
Datos e Información Complentaria [D]	Es la materialización de la información.
Claves criptográficas [K]	Permiten la protección de las partes o secretos de la organización; son fundamentales para asegurar el correcto funcionamiento de los mecanismos criptográficos.
Servicios [S]	Mejor conocidos como servicios auxiliares, los cuales ayudan en la organización del sistema.
Aplicaciones informáticas [SW]	Es el *software* del sistema que facilita el manejo de la información.
Equipos informáticos [HW]	Es el *hardware* donde se procesan las aplicaciones, datos y servicios.
Soportes de información [Media]	Son los instrumentos donde se almacenan los datos y/o información.
Equipamiento auxiliar [AUX]	Son los equipos que completan el material informático.
Redes de comunicaciones [COM]	Son el conjunto de medios de transmisión y elementos que permiten el intercambio de la información.
Instalaciones [L]	Es el lugar donde se montan los equipos informáticos y de comunicaciones.
Personas [P]	Son quienes hacen uso de todos los componentes que previamente se han mencionado.

1.3.5.1.2. Valoración de Activos

Los activos se miden por el valor que tienen en la organización, para lo cual, existen varios parámetros para la valoración de los activos en cada dimensión de seguridad. El objetivo

principal de ejecutar una valoración de activos es obtener una mejor aproximación de las consecuencias que se darían si las amenazas llegaran a materializarse; en otras palabras, es medir que tan dañina puede ser una amenaza en los activos en base a cierta dimensión [10].



valor		*criterio*
10	extremo	daño extremadamente grave
9	muy alto	daño muy grave
6-8	alto	daño grave
3-5	medio	daño importante
1-2	bajo	daño menor
0	despreciable	irrelevante a efectos prácticos

Figura 1.6. Escala de valoración de activos en MAGERIT *[11]*

En la **Figura 1.6** se puede observar una escala de valoración de activos, la misma que se utiliza a manera de ejemplo para definir otras escalas en función de los criterios y requerimientos de la empresa.

1.3.5.2. Amenazas

1.3.5.2.1. Identificación de amenazas

Las amenazas son consideradas como causas potenciales de los incidentes que pueden ocasionar daños en los sistemas de información de las organizaciones.

Para la identificación de amenazas, la metodología MAGERIT en su libro II presenta un catálogo de amenazas, que están clasificadas en cuatro tipos como se describen a continuación [11]:

- **[N] Desastres naturales:** Son considerados los accidentes naturales; los sistemas de información son víctimas pasivas, sin embargo, se los debe tomar en cuenta. En la **Tabla 1.3** se muestra la lista de amenazas correspondientes a este tipo [11].

Tabla 1.3. Clasificación de amenazas relacionada a Desastres Naturales

5.1. [N] Desastres naturales
5.1.1. [N.1] Fuego
5.1.2. [N.2] Daños por agua
5.1.3. [N.*] Desastres naturales

- **[I] De origen industrial:** También conocidos como “de entorno”, al igual que el caso anterior los sistemas son víctimas pasivas y podrían ser la contaminación, fallos eléctricos [11], así como se muestra en la **Tabla 1.4.**

Tabla 1.4. Clasificación de amenazas relacionada a Origen Industrial

5.2. [I] De origen industrial
5.2.1. [I.1] Fuego
5.2.2. [I.2] Daños por agua
5.2.3. [I.*] Desastres industriales
5.2.4. [I.3] Contaminación mecánica
5.2.5. [I.4] Contaminación electromagnética
5.2.6. [I.5] Avería de origen físico o lógico
5.2.7. [I.6] Corte del suministro eléctrico
5.2.8. [I.7] Condiciones inadecuadas de temperatura o humedad
5.2.9. [I.8] Fallo de servicios de comunicaciones
5.2.10. [I.9] Interrupción de otros servicios y suministros esenciales
5.2.11. [I.10] Degradación de los soportes de almacenamiento de la información
5.2.12. [I.11] Emanaciones electromagnéticas

- **[E] Errores y fallos no intencionados:** Se dan por errores u omisiones no intencionales por parte de las personas en el sistema de información. En la **Tabla 1.5** se muestra una lista de amenazas [11]**.**

Tabla 1.5. Clasificación de amenazas relacionada a Errores y Fallos no intencionados

5.3. [E] Errores y fallos no intencionados	
5.3.1. [E.1] Errores de los usuarios	5.3.10. [E.15] Alteración accidental de la información
5.3.2. [E.2] Errores del administrador	5.3.11. [E.18] Destrucción de información
5.3.3. [E.3] Errores de monitorización (log)	5.3.12. [E.19] Fugas de información
5.3.4. [E.4] Errores de configuración	5.3.13. [E.20] Vulnerabilidades de los programas (software)
5.3.5. [E.7] Deficiencias en la organización	5.3.14. [E.21] Errores de mantenimiento / actualización de programas (software)
5.3.6. [E.8] Difusión de software dañino	5.3.15. [E.23] Errores de mantenimiento / actualización de equipos (hardware)
5.3.7. [E.9] Errores de [re-]encaminamiento	5.3.16. [E.24] Caída del sistema por agotamiento de recursos
5.3.8. [E.10] Errores de secuencia	5.3.17. [E.25] Pérdida de equipos
5.3.9. [E.14] Escapes de información	5.3.18. [E.28] Indisponibilidad del personal

- **[A] Ataques intencionados:** Causadas por las personas de forma deliberada. A diferencia de los anteriores, son realizadas intencionalmente por parte del personal para ocasionar problemas donde puedan obtener un beneficio personal o causar perjuicios o daños a los propietarios de la organización, como se muestra en la **Tabla *1.6*** [11]

Tabla 1.6. Clasificación de amenazas relacionada a ataques intencionados

5.4. [A] Ataques intencionados	
5.4.1. [A.3] Manipulación de los registros de actividad (log)	5.4.13. [A.15] Modificación deliberada de la información
5.4.2. [A.4] Manipulación de la configuración	5.4.14. [A.18] Destrucción de información
5.4.3. [A.5] Suplantación de la identidad del usuario	5.4.15. [A.19] Divulgación de información
5.4.4. [A.6] Abuso de privilegios de acceso	5.4.16. [A.22] Manipulación de programas
5.4.5. [A.7] Uso no previsto	5.4.17. [A.23] Manipulación de los equipos
5.4.6. [A.8] Difusión de software dañino	5.4.18. [A.24] Denegación de servicio
5.4.7. [A.9] [Re-]encaminamiento de mensajes	5.4.19. [A.25] Robo
5.4.8. [A.10] Alteración de secuencia	5.4.20. [A.26] Ataque destructivo
5.4.9. [A.11] Acceso no autorizado	5.4.21. [A.27] Ocupación enemiga
5.4.10. [A.12] Análisis de tráfico	5.4.22. [A.28] Indisponibilidad del personal
5.4.11. [A.13] Repudio	5.4.23. [A.29] Extorsión
5.4.12. [A.14] Interceptación de información (escucha)	5.4.24. [A.30] Ingeniería social (picaresca)

1.3.5.2.2. Valoración de amenazas

Para la valoración de las amenazas se debe considerar, la degradación que indica el perjuicio que tendría un activo en el supuesto que ocurriera, y la probabilidad que pueda tomar cuerpo la amenaza [10].

Tabla 1.7. Degradación del valor y probabilidad de ocurrencia según MAGERIT

VALORACIÓN DE LA DEGRADACIÓN DEL VALOR				**VALORACIÓN DE LA PROBABILIDAD DE OCURRENCIA**			
MA	muy alta	casi seguro	Fácil	MA	100	muy frecuente	a diario
A	Alta	muy alto	Medio	A	10	Frecuente	Mensualmente
M	Media	Posible	Difícil	M	1	Normal	una vez al año
B	Baja	poco probable	muy difícil	B	1/10	poco frecuente	cada varios años
MB	muy baja	muy raro	extremadamente difícil	MB	1/100	muy poco frecuente	Siglos

De manera más explícita, la degradación del valor es la medida del daño causado por el incidente en caso de que pueda ocurrir; suele ser caracterizado como una fracción del valor del activo. Se tienen dos escenarios, cuando la amenaza no es intencional es suficiente saber la fracción perjudicada físicamente del activo para realizar el cálculo proporcional a lo que se pierde; cuando la amenaza es intencional, no se puede medir la proporcionalidad

del daño puesto que el atacante lo realiza de forma selectiva pudiendo causar muchísimo daño. En la **Tabla 1.7** se puede observar un modelo de cómo valorar la degradación del valor.

Por otro lado, se tiene la probabilidad de ocurrencia, la cual es más compleja de expresar; en ocasiones se la modela en una escala nominal, numéricamente se la puede representar como una frecuencia de ocurrencia, en la cual se toma como base un año, de tal forma que la tasa anual de ocurrencia se toma como una medida de la probabilidad de que algo suceda [10]**.**

1.3.5.3. Impacto Potencial

1.3.5.3.1. Valoración del Impacto Potencial

Se considera como impacto a la dimensión que causa daño sobre un activo originado de la materialización de una amenaza; una vez que se conoce el valor de los activos estudiados en varias dimensiones y la degradación que ocasionan las amenazas, se puede estimar el impacto que se genera, a través del producto del valor del activo por el nivel de degradación en cada dimensión [18].

Finalmente, se debe sumar el Impacto Potencial obtenido en cada dimensión y así obtener el Impacto Potencial total de un activo. Además, se establece una escala de referencia para la valoración del Impacto Potencial por dimensiones y el Impacto Potencial total, como se muestra en la **Tabla 1.8.**

Tabla 1.8. Escala de valoración del Impacto Potencial

IMPACTO POTENCIAL	
1	Muy bajo
2	Bajo
3	Moderado
4	Alto
5	Muy alto

1.3.5.4. Riesgo Potencial

1.3.5.4.1. Valoración del Riesgo Potencial

Se define riesgo como la medida del daño probable sobre un activo, si se conoce el Impacto Potencial de las amenazas sobre los activos es fácil estimar el riesgo en base a la probabilidad de ocurrencia. A medida que crece el impacto y la probabilidad, el riesgo también lo hace, siendo proporcional [18].

A continuación, se describen las cuatro zonas que se pueden apreciar en el modelo de la **Figura 1.7**:

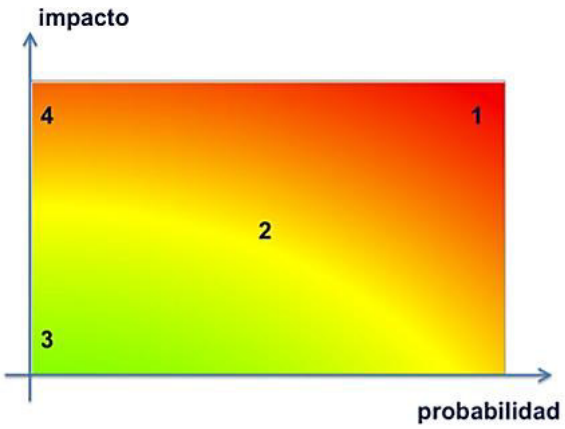


Figura 1.7. Riesgo en función del impacto y la probabilidad *[10]*

Zona 1: Zona de color rojo donde se reflejan riesgos de alta probabilidad de ocurrencia y de consecuencias de gran impacto.

Zona 2: Zona de color amarillo donde abarca un amplio rango de situaciones, desde situaciones improbables y de impacto medio hasta situaciones con alta probabilidad de ocurrencia, pero de bajo o muy bajo impacto.

Zona 3: Zona de color verde donde los riesgos no son muy probables y en caso de ejecutarse son de bajo impacto.

Zona 4: Zona de color naranja donde los riesgos no son muy probables, pero tienen alto impacto.

Además, se establece una escala de referencia para la valoración del Riesgo Potencial en cada dimensión y el Riesgo Potencial total. Dicha escala permite la representación de los resultados numéricos y por niveles de complejidad, como se indica en la **Tabla 1.9**.

Tabla 1.9. Escala de valoración Riesgo Potencial

RIESGO POTENCIAL	
1	Muy bajo
2	Bajo
3	Moderado
4	Alto
5	Muy alto

1.3.5.5. Documento de Aplicabilidad

De las siglas en inglés *Statement of Applicability* (SoA), el documento de aplicabilidad es un compilado de 114 controles de seguridad asociado y 35 objetivos de control establecidos en el Anexo A de la norma ISO/IEC 27001. Se lo utiliza como una referencia para la implementación de medidas de seguridad de la información y verificar que se tomen en cuenta todas las medidas de protección que no se habían considerado antes en la organización [19].

1.3.5.6. Controles o Salvaguardas

Es de vital importancia medir los riesgos e impactos a los que se exponen los activos si no se tuviera ningún tipo de protección; en la práctica no se encuentran sistemas sin protección, por lo que se introduce este concepto de controles o salvaguardas [11].

Las salvaguardas o también conocidas como contramedidas son procedimientos (o mecanismos tecnológicos) que minimizan el riesgo, dicho de otra manera, permiten hacer frente a las amenazas. Dependiendo del escenario las amenazas se pueden reducir únicamente con una correcta organización; en algunos casos se necesita de *hardware* o *software* especializado; en otros depende de la seguridad física y finalmente de una correcta aplicación de las políticas del personal [11].

Existen muchos tipos de salvaguardas para tomar en cuenta, por lo cual es crítico realizar una selección de aquellas que son más relevantes considerando lo que se debe proteger. En tal virtud se deben considerar los siguientes aspectos:

1. Clase de activos, puesto que cada activo tiene una manera específica de protección.
2. Dimensiones de la seguridad que necesitan la protección.
3. Amenazas que hay que enfrentar.
4. Salvaguardas alternativas en caso de su existencia

Además de todo lo mencionado, hay que considerar: el valor de los activos (centrando la atención en el activo más importante y apartando lo irrelevante); la probabilidad de que la amenaza se materialice (considerando los riesgos más importantes); y, qué tanto podrían cubrir las salvaguardas alternativas, en caso de implementarse.

1.3.5.7. Grado de madurez o eficacia de los controles

El grado de eficacia es el valor que mide la eficacia del control existente o establecido sobre un activo frente al riesgo que protege.

La valoración de la eficacia considera dos puntos de vista, el técnico y la operación de la salvaguarda. Desde el punto de vista técnico las salvaguardas son técnicamente adecuadas para enfrentar el riesgo al que se expone y siempre se las emplea. Desde el punto de vista de operación de la salvaguarda, esta se encuentra perfectamente desplegada, configurada y mantenida; los usuarios tienen la formación y conciencia para operar; hay procedimientos concisos de uso habitual y en caso de emergencia, y existen controles (pueden ser alarmas) que notifican posibles fallos en el sistema. Para decir que una salvaguarda sea 100 % eficaz se requiere que cumpla con los dos puntos de vista.

En la **Tabla 1.10** se puede observar la escala de cómo representar el nivel en el que se encuentran las salvaguardas en el sistema; conocido esto se puede evaluar de nuevo y tomar mejores precauciones o en caso de ser necesario implementar otros tipos de salvaguardas para afrontar los riesgos a los cuales están sometidos los activos [10].

Tabla 1.10. Escala de niveles de madurez de los controles

MADUREZ O EFICACIA DE LOS CONTROLES			
PUNTOS-RIESGO	**NIVEL**	**FACTOR**	**DESCRIPCIÓN**
0	L0	0%	Inexistente
1	L1	20%	Inicial
2	L2	40%	Reproducible pero intuitivo
3	L3	60%	Proceso definido
4	L4	80%	Gestionable y medible
5	L5	100%	Optimizado

Una eficacia del *0%* significa que no existen salvaguardas desplegadas, en tanto que una eficacia del *100%* indica que las salvaguardas implementadas son las más adecuadas para los requerimientos del sistema y soporta bastante bien los riesgos a los cuales se enfrenta [10].

1.3.5.8. Riesgo Actual

Se denomina Riesgo Actual a la medida del daño que puede ocasionar a un activo de la empresa; se lo obtiene a partir del Riesgo Potencial y en función del nivel de madurez de los controles existentes, en el caso de que éstos existan [10].

El Riesgo Actual será igual al Riesgo Potencial en el caso de que la empresa no tenga ningún control existente en el sistema de seguridad de la información.

1.3.5.9. Aceptación y tratamiento del riesgo

Una vez realizado el análisis y evaluación del riesgo, procede la aceptación y tratamiento del riesgo. Por lo tanto, se debe realizar el proceso en dos fases, la aceptación del riesgo y el tratamiento del riesgo. En la **Figura 1.8** se pueden apreciar las posibles decisiones a tomarse después de haber realizado el estudio de los riesgos.

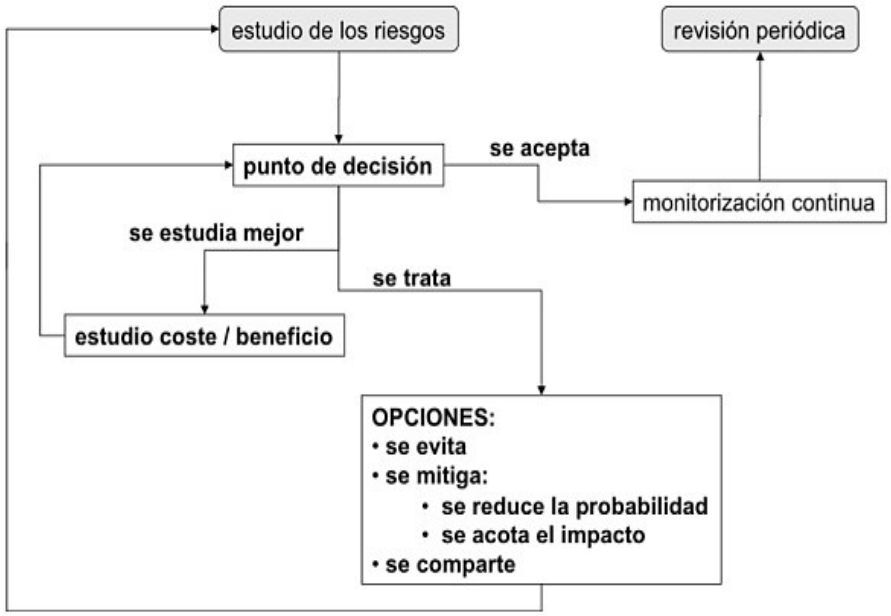


Figura 1.8. Decisiones de tratamiento de los riesgos [10]

Para cada riesgo se puede asumir una calificación en base a las consideraciones tomadas en cuenta en el estudio de los impactos y riesgos a los que está expuesto el sistema, por lo que se tienen las siguientes categorías:

- **Crítico:** Requiere atención urgente
- **Grave:** Requiere atención
- **Apreciable:** Puede ser objeto de estudio para su tratamiento
- **Asumible:** No hay toma de acciones para contenerlo
-

1.3.5.9.1. Aceptación del riesgo

La aceptación del riesgo se basa en los valores resultantes del Riesgo Actual en cada dimensión de seguridad, del Riesgo Actual total y del criterio de la alta dirección. Después de haber realizado este análisis, se pueden definir dos niveles de riesgo: aceptable e inaceptable.

Se dice que un nivel de riesgo es aceptable cuando es bajo o despreciable, muy bajo o insignificante, por lo que no es necesario instaurar salvaguardas adicionales. Sin embargo, se realiza el monitoreo continuo y revisión regular de los riesgos.

Por otro lado, se dice que un nivel de riesgo es inaceptable si es medio, alto y muy alto, para lo cual se deben tomar las opciones del tratamiento del riesgo que se indican en las siguientes secciones [17].

1.3.5.9.2. Tratamiento del riesgo

En primer lugar, se debe tener un listado de riesgos que son categorizados por prioridades en base a criterios de evaluación del riesgo y la relación con los escenarios del incidente que llevan a dichos riesgos [17].

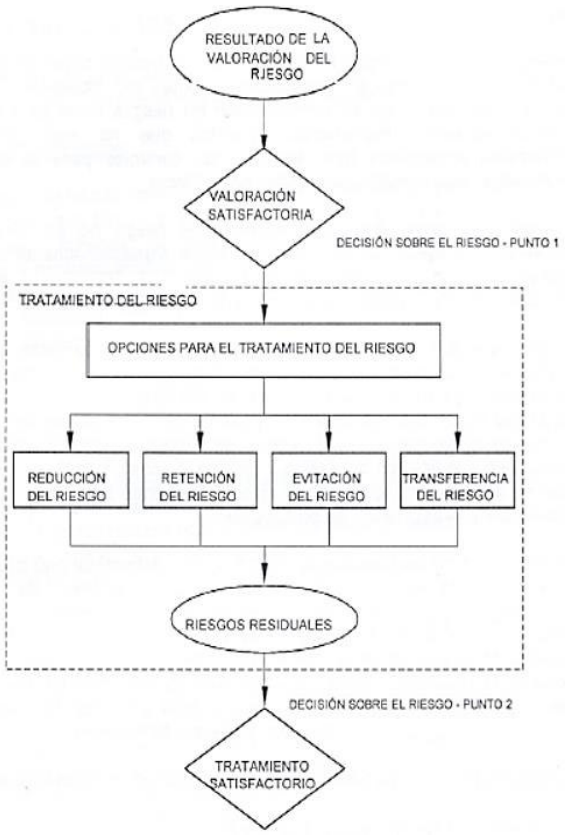


Figura 1.9. Actividad para el tratamiento del riesgo [17]

Para el tratamiento del riesgo se dispone de cuatro opciones como se puede apreciar en la **Figura 1.9**. Estas opciones deben seleccionarse en base al resultado de la valoración del riesgo, el costo esperado para implementar dichas opciones y los beneficios que se espera como resultado de las opciones; además, no son mutuamente excluyentes lo que significa que se puede hacer una combinación de ellas para un tratamiento más eficaz del riesgo [17].

En las siguientes secciones se describen de mejor forma las opciones que se tiene para el tratamiento del riesgo.

1.3.5.9.3. Reducción del riesgo

Para empezar el nivel de riesgo se debería minimizar en la selección de controles, de tal forma que el Riesgo Actual se pueda volver a evaluar y considerar como aceptable.

Es recomendable la selección de controles adecuados y debidamente justificados que cumplan los requisitos que se identifican en la valoración y tratamiento del riesgo. Esta selección debe considerar los criterios de aceptación del riesgo, además, requisitos legales, reglamentarios y contractuales; también, se debe tomar en cuenta los costos y el tiempo para la implementación de controles. Entre las funciones de protección más importantes que brindan los controles se encuentran: corrección, eliminación, prevención, disuasión, detección, minimización del impacto, recuperación, monitoreo y toma de conciencia [17].

Por otro lado, pueden existir restricciones que pueden afectar la selección de controles, como indica el **Anexo F** de la ISO/IEC:27005:2012, entre las más comunes se tienen [17]:

- Restricciones de tiempo: Establecer periodos de tiempo aceptables.
- Restricciones financieras: No deben ser costos en la implementación.
- Restricciones técnicas: Pueden tener problemas de compatibilidad de programas.
- Restricciones operativas: Puede ser necesario el trabajo 24/7 y generar más costos.
- Restricciones culturales: Pueden depender de la cultura y creencias del personal.
- Restricciones éticas: Dependen de la ética de las personas en cada país.
- Restricciones ambientales: Se deben a las condiciones climáticas y geográficas.
- Restricciones legales: Pueden existir leyes que incluyan la protección de datos.
- Restricciones de facilidad de uso: Deben ser fáciles de usar y óptimos en el tiempo.

- Restricciones de personal: Puede ser costosa el nivel de experiencia del personal.
- Restricciones para la integración de controles nuevos y existentes: Incompatibilidad

1.3.5.9.4. Retención o aceptación del riesgo

La aceptación del riesgo sin acción posterior se debe tomar en base a la evaluación de este; si el nivel de riesgo cumple con los criterios para su aceptación, no se necesita la implementación de controles adicionales, en esas condiciones el riesgo se podría retener [17].

1.3.5.9.5. Evitación del riesgo

Se debe evitar las acciones o actividades donde se origina un riesgo particular. Para el caso donde los riesgos considerados muy altos y/o los costos de implementación de otras opciones de tratamiento del riesgo sobrepasan los beneficios, se puede tomar la decisión de evitar completamente el riesgo, a través del cese de una o varias actividades planificadas o existentes, o por medio del cambio de condiciones donde se ejecuta tales actividades [17].

1.3.5.9.6. Transferencia del riesgo

En esta opción se debería transferir el riesgo a otro sitio donde se pueda gestionar de forma más eficaz un riesgo después de la evaluación de este. Muchas veces la transferencia del riesgo implica compartir el riesgo con externos, sin embargo, esto puede conllevar la creación de nuevos riesgos o la modificación de riesgos ya identificados, para lo cual se debe realizar un tratamiento adicional del riesgo [17].

1.3.5.10. Riesgo Planificado

Se denomina Riesgo Planificado a la medida del Riesgo Actual con su respectivo tratamiento, el mismo que en un lapso de implementación se verá afectado y disminuirá en función del nivel de madurez de los controles establecidos [17].

2. METODOLOGÍA

El presente proyecto de titulación plantea realizar el diseño del Sistema de Gestión de la Seguridad de la Información (SGSI) para la empresa Curtiembre Quisapincha ubicada en la provincia de Tungurahua.

El método desarrollado para el presente trabajo de titulación engloba las cláusulas mandatorias que permiten validar el cumplimiento del SGSI y una metodología de análisis de gestión de riesgos.

Según la norma ISO 27001:2013 se indica que consta de siete cláusulas mandatorias, de las cuales, tan como se lo señaló en el capítulo 1, únicamente se desarrollarán las relacionadas a Contexto de la Organización, Liderazgo y Planificación, que tienen su enfoque en la fase de diseño del SGSI.

En la **Figura 2.1** se indican los ítems a tratar en las tres cláusulas mandatorias.

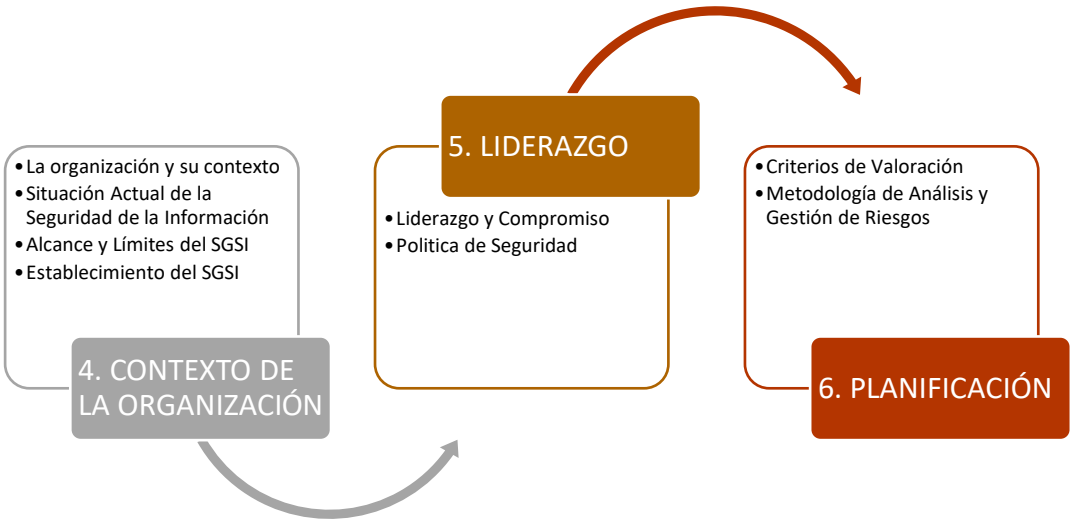


Figura 2.1. Cláusulas mandatorias del SGSI

Además, en la **Figura 2.2** para el cumplimiento de la cláusula de Planificación se usará parte de la metodología MAGERIT v3 y la norma ISO 27001:2013, para el establecimiento de una metodología de análisis y gestión de riesgos en función de los requerimientos de la empresa. Así también, se muestra un esquema que permitirá una mejor comprensión de la metodología utilizada en el presente trabajo.

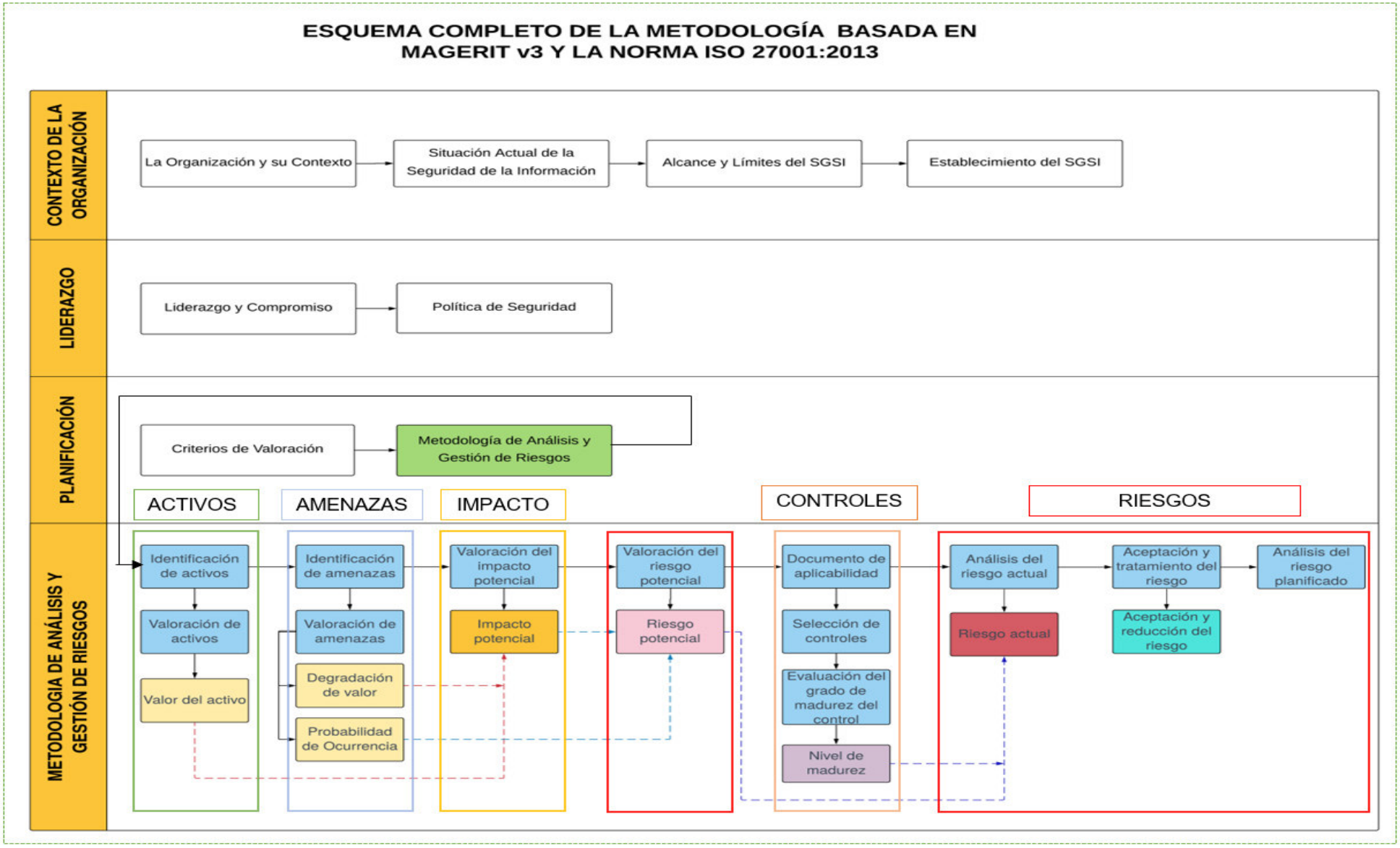


Figura 2.2. Esquema completo de la metodología

2.1. CONTEXTO DE LA ORGANIZACIÓN

El contexto de la organización se refiere a los factores internos y externos relevantes para el propósito de la empresa y en qué medida afectan a la capacidad para el cumplimiento de resultados deseados del SGSI [14]. Entre los ítems a tratar se tienen cultura y estructura organizacional, infraestructura tecnológica, situación actual de la seguridad de la información; y alcance, límites y establecimiento del SGSI.

2.1.1. LA ORGANIZACIÓN Y SU CONTEXTO

2.1.1.1. Historia de la empresa

Curtiembre Quisapincha es una empresa familiar que inició sus actividades en el año 1999 en la Parroquia Quisapincha del cantón Ambato. La misma se dedica a la producción de cuero y a la fabricación de calzado y productos terminados en cuero.

La empresa se ha ido consolidando a través de los años, convirtiéndose en una firma de renombre en el mercado nacional e internacional. La calidad de sus productos y el constante desarrollo tecnológico e innovación en los productos que maneja, ha conquistado las preferencias de un exigente mercado [20]**.**

Este trabajo lo ha logrado gracias a la calidad de mano de obra de su recurso humano, pues ha sido un factor fundamental para el éxito alcanzado en la empresa, además ha permitido que la empresa enfrente los constantes retos del futuro con mayor eficacia.

2.1.1.2. Misión

“La misión de la empresa es producir, innovar y comercializar una extensa diversidad de cuero y productos manufacturados de calidad y excelencia, amigables con el medio ambiente, para satisfacer las necesidades de clientes nacionales e internacionales. Contribuyendo de tal manera al desarrollo del país y brindando una gran satisfacción al cliente” [20].

2.1.1.3. Visión

“Impulsar el desarrollo de productos para ser líderes en el mercado nacional e internacional en la producción de cuero y productos manufacturados, así como el turismo” [20].

2.1.1.4. Valores

Los valores de la empresa son los siguientes [20]:

- Honestidad

- Puntualidad
- Responsabilidad
- Justicia
- Innovación
- Comunicación
- Compromiso

2.1.2. ESTRUCTURA ORGANIZACIONAL

La empresa se encuentra dividida por áreas y distribuida de manera jerárquica en función de sus necesidades, como se muestra en la **Figura 2.3**. En el primer nivel jerárquico se tiene el área fundamental de Gerencia General; en el segundo nivel se tienen 6 áreas distribuidas estratégicamente para la supervisión del tercer nivel jerárquico. El tercer nivel se distribuye por departamentos y fases para el desarrollo de todos los procesos internos de la empresa [21].

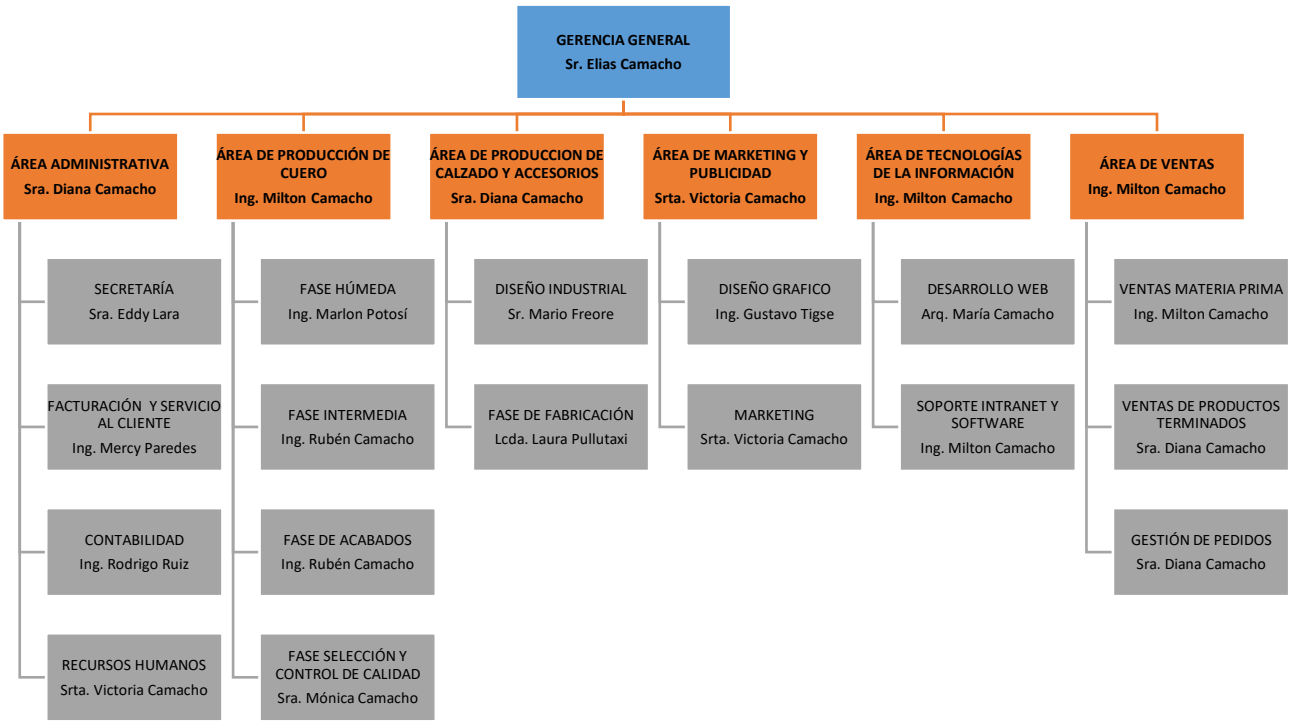


Figura 2.3. Estructura Organizacional Curtiembre Quisapincha

A continuación, se explica la función de cada área de la estructura organizacional.

2.1.2.1. Gerente General

Esta área es la base fundamental de la empresa, porque es la responsable de la autorización y supervisión de todos los procesos internos y externos de la organización, en el ámbito legal e institucional [21].

A continuación, se detallan algunas de las funciones principales de esta área:

- Gestión y control de acceso a cuentas bancarias.
- Autorización de pagos a proveedores y nómina de empleados.
- Supervisión de balances mensuales y anuales.
- Autorización de procesos internos y externos de la empresa.
- Autorización de importaciones y exportaciones.
- Supervisión de jefes de área.
- Autorización para compras de insumos e inmuebles corporativos.
- Supervisión de procesos en el área de producción de cuero.

2.1.2.2. Área Administrativa

Tiene como objetivo principal el control y supervisión de todos los procesos contables e internos de la empresa. A continuación, se detallan las funciones principales de esta área [21]:

- Supervisión de todas las tareas realizadas por el departamento de Secretaría.
- Supervisión de todas las tareas realizadas por el departamento de Facturación y atención al cliente.
- Supervisión del departamento de Contabilidad.
- Supervisión del departamento de Recursos Humanos.
- Análisis y gestión de balances mensuales.

2.1.2.3. Área de Producción de Cuero

Esta área tiene como objetivo, supervisar todos los subprocesos de producción del cuero. Algunas de las funciones principales de esta área se listan a continuación [21]:

- Supervisión de tiempos y cronogramas establecidos según cada subproceso.
- Distribución de actividades diarias, semanales y mensuales para el proceso de producción.
- Planificación de tiempos de entrega del producto terminado.
- Supervisión de las fichas técnicas de los productos y formulaciones químicas para cada proceso.
- Supervisión y control de calidad en la fase final del proceso de producción.

2.1.2.4. Área de Producción de Calzado y Accesorios

Esta área fue definida con el objetivo de supervisar todos los subprocesos de producción del calzado, chaquetas, carteras y demás accesorios elaborados en cuero; algunas de sus principales funciones son [21]:

- Aprobación de diseños y nuevas colecciones.
- Supervisión de la calidad del cuero para la fabricación del calzado.
- Supervisión del corte, destallado, aparado, armado, plantado y pulido del calzado.
- Control de calidad del calzado.
- Supervisión de la producción semanal y mensual del calzado.
- Supervisión de los insumos y materia prima para la elaboración de chaquetas, carteras y demás accesorios.

2.1.2.5. Área de Marketing y Publicidad

Área creada con el objetivo de renovar la imagen de la empresa; es un área completamente nueva, tiene varias funciones como las que se detallan a continuación [21]:

- Supervisión y autorización de todos los diseños elaborados por el departamento de Diseño Gráfico.
- Planificación de las sesiones fotográficas con nuevos productos y nuevas colecciones.
- Gestión de recursos para la elaboración e impresión de *banners* publicitarios físicos y virtuales.
- Supervisión del plan estratégico de *marketing* elaborado por el departamento de *Marketing.*

- Asignación del presupuesto mensual para lanzamiento de publicidad en el sitio web, tienda virtual y redes sociales.

2.1.2.6. Área de Tecnologías de la Información

Área creada con el fin de brindar una infraestructura tecnológica estable dentro de la empresa; años más tarde se volvió indispensable debido a que todo el sistema de ventas está canalizado por medios digitales y a su vez dicho sistema consume servicios de proveedores externos [21].

La tienda virtual, sitio web y redes sociales son medios digitales, a través de los cuales la empresa ofrece sus productos, por lo tanto, deben ser canales de distribución seguros y confiables para los consumidores.

Las funciones principales de esta área son:

- Soporte y mantenimiento de la infraestructura de red interna de la empresa, realizada por el departamento de Soporte Intranet y Software.
- Configuración y gestión de control de acceso de los equipos o dispositivos electrónicos.
- Administración del sitio web mediante CSS (Cascading Style Sheets), CSV (Comma- Separated Values) y JavaScript[7].
- Supervisión del correcto funcionamiento de las cámaras de vigilancia.
- Gestión y generación de *backup* de la información y base de datos de la empresa.
- Gestión y administración de los servidores físicos y virtuales de la empresa.
- Gestión de seguridad y confidencialidad de datos de la cartera de clientes de la empresa.

2.1.2.7. Área de Ventas

Es una área estratégica y fundamental de la empresa, porque en base a ésta se encuentra el giro del negocio de la empresa. Las funciones principales de esta área son [21]:

- Creación de una cartera de clientes para distribución de productos.
- Atención al cliente presencial y en línea.
- Gestión de pedidos.

[7] JavaScript: Es un lenguaje de programación de *scripts,* utilizado en las páginas web.

- Seguimiento de pedidos en producción.
- Ingreso de nuevos clientes.
- Análisis y gestión de ventas semanales y mensuales.
- Control de calidad de salida de productos.
- Supervisión de embalaje y presentación del producto.
- Gestión de vendedores en función de la meta establecida.

2.1.3. INFRAESTRUCTURA TECNOLÓGICA

Se revisará la infraestructura tecnológica de la empresa, con el fin de realizar el análisis de cada uno de los activos de la empresa.

2.1.3.1. Información

La información es considerada como el activo esencial que la empresa emplea en el giro de negocio y es fundamental para cumplir con los objetivos de la empresa. Además, se dispone de una amplia base de datos que contiene datos personales de los clientes y proveedores [22].

2.1.3.2. Hardware

2.1.3.2.1. Servidor físico HP Proliant DL 360P

Un servidor físico es un ordenador diseñado para ofrecer servicios a través de una arquitectura cliente - servidor o un modelo de red *peer to peer* [23].

La empresa utiliza un servidor físico HP[8] Proliant[9] similar al que se muestra en la **Figura 2.4**, con arquitectura cliente-servidor; en este equipo se alojan varios servidores virtuales.

Figura 2.4. Servidor HP DL360P [23]

[8] HP: Hewlett-Packard empresa de tecnología estadounidense.
[9] Proliant: Marca de hardware para servidores comercializada actualmente por HP Enterprise.

Las características de este servidor se indican en la **Tabla 2.1.**

Tabla 2.1. Características del Servidor HP Proliant DL 360P

CARACTERÍSTICAS DEL EQUIPO	
MARCA:	HP Proliant
MODELO:	DL 360P G8
PROCESADORES:	2- INTEL XEON E5-2603V2
MEMORIA RAM:	32 GB
DISCO DURO:	HP SAS - 1GB
CPU:	2.3 GHz

2.1.3.2.2. Entorno de virtualización de Servidores PROXMOX

Sobre el servidor físico se ejecuta la plataforma de virtualización PROXMOX, la cual permite la ejecución de diversos servicios o aplicativos a través de máquinas virtuales [24]. Un servidor virtual es la simulación de un servidor físico en un ambiente virtual, es decir, realiza sus mismas funciones; se diferencia en que, en lugar de tener solo un servidor físico en una máquina física, se pueden alojar varios servidores virtuales en dicha máquina [25].

Cada servidor virtual tiene asignada una funcionalidad diferente, de tal manera que operan como servidores independientes y se los puede ejecutar de forma paralela para mayor aprovechamiento de recursos de una sola máquina física [25].

PROXMOX es un entorno de virtualización de código abierto basado en Debian; permite la gestión de máquinas virtuales tanto de Linux como Windows y contenedores [26].

La empresa utiliza dicho entorno para la administración y gestión de sus servidores virtuales, debido a que este entorno de virtualización posee ciertas características que brindan mayor confiabilidad.

Entre las características principales de PROXMOX se tienen [27]:

- Posee una interfaz Web como se indica en la **Figura 2.5**.
- Permite realizar migración en vivo.
- Es una aplicación de código abierto.
- Es gratuito.
- Posee herramientas de línea de comandos

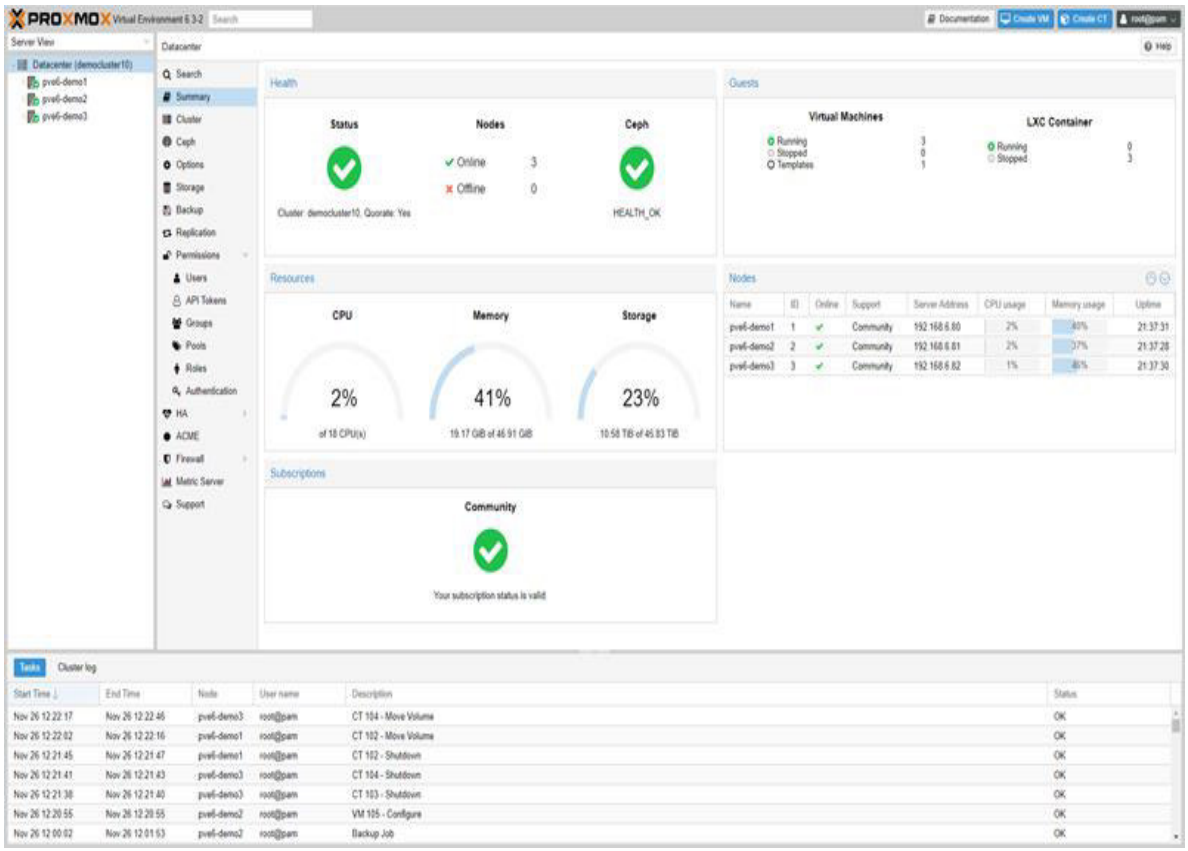


Figura 2.5. Interfaz Web PROXMOX [28]

El sistema operativo utilizado para el despliegue de los diferentes servicios virtualizados es CentOS 8, que es uno de los sistemas Linux más estable, confiable, seguro, de alto rendimiento y libre de errores. Este sistema operativo es ideal para servidores, está basado en RHEL (Red Hat Enterprise Linux) que es una de las mejores distribuciones para servidores [28].

A continuación, se listan los servidores virtualizados:

- Servidor DNS (Domain Name System)
- Servidor de Base de Datos Oracle XE 18c
- Servidor de Base de Datos MySQL 8.0 (My Structured Query Language)
- Servidor de Base de Datos PostgreSQL 13
- Servidor OwnCloud
- Servidor FTP (File Transfer Protocol)
- Servidor Web NGINX

2.1.3.2.3. Switches

Son dispositivos que sirven para conectar equipos en una Red de Área Local (LAN), que permite la interconectividad en un área específica [29].

Los *switches* TP-LINK, Modelo TL-SG1024D son no administrables, su característica principal es que tiene un sistema *plug and play* y es uno de los más comunes en intranets de oficinas pequeñas. Cuenta con 24 Puertos Gigabit Ethernet como se indica en la **Figura 2.6**.

Figura 2.6. Switch TP-LINK [30]

La empresa cuenta con dos *switches* de marca TP-LINK con características que se indican en la **Tabla 2.2**; que son los principales que están ubicados en el *rack* del Área de Tecnologías de la Información. Y también cuenta con ocho switches secundarios distribuidos en varias áreas de la empresa, los cuales se listan en la **Tabla 2.3**.

Tabla 2.2. Características del Switch

CARACTERÍSTICAS DEL EQUIPO	
MARCA:	TP-LINK
MODELO:	TL-SG1024D
PUERTOS RJ-45:	en24
RED:	Gigabit Ethernet
TECNOLOGÍA:	Plug and Play

Tabla 2.3. Switches por áreas

SWITCHES			
ÁREA	**CANTIDAD**	**EQUIPO**	**CARACTERÍSTICAS**
Área de Tecnologías de la Información	2	*SWITCH*	MARCA:TP-LINK MODELO: TL-SG1024D
Área Administrativa	1	*SWITCH*	MARCA: INTELBRAS MODELO: ITC4100
	1	*SWITCH*	MARCA: NAXOS800 MODELO: ASIDTOB4U3
	1	*SWITCH*	MARCA: NWAY MODELO: ENH908-NWY
Área de Ventas	2	*SWITCH*	MARCA: DLINK MODELO: DAP1360
	1	*SWITCH*	MARCA: DLINK MODELO: DAP1360

2.1.3.2.4. Router ONT

La empresa cuenta con un r*outer* ONT Huawei, modelo HG8646M (Terminal de Red Óptica, ver **Figura 2.7**), que permite la conectividad a Internet a través de fibra óptica desde el proveedor de servicios hasta la red interna.

Figura 2.7. Router ONT Huawei HG8546M

Las especificaciones técnicas del *Router* ONT, se las puede observar en la **Tabla 2.4**.

Tabla 2.4. Características del Router ONT

CARACTERÍSTICAS DEL EQUIPO	
MARCA:	HUAWEI
MODELO:	HG8546M
PUERTOS RJ-45:	3
PUERTO RJ-11:	1
PUERTO USB:	1
WIFI:	2.4 GHz- V.300 Mbps
CONECTIVIDAD:	Alámbrico/ Inalámbrica
TECNOLOGÍA:	GPON[10]
CONECTORES:	SC: *Suscriber Conector* UPC: *Ultra Physical Contact*

2.1.3.2.5. Computadoras de Escritorio

La empresa cuenta con 9 computadoras de escritorio, con CPUs de características afines a las actividades de cada área como se muestra en la **Tabla 2.5** y que se describen en los siguientes párrafos.

En el Área de Gerencia General se dispone de una computadora que permite el acceso a la red interna, al sistema contable y a las cuentas bancarias a través de Internet.

En el Área Administrativa existen tres computadoras distribuidas para las sub-áreas que corresponden a: Secretaría, Facturación y servicio al cliente, Contabilidad y Recursos Humanos.

El Área de Producción de Cuero usa dos computadoras para estrictamente el manejo y administración de información confidencial referente a patentes de formulaciones químicas para la producción del cuero, así también para el inventario y Kardex diario de producción de cuero y productos químicos.

[10] GPON: *Gigabit-capable Passive Optical Network*/ Red Óptica Pasiva con capacidad Gigabit.

Finalmente, el Área de Ventas cuenta con tres computadoras designadas para el acceso a las bases de datos de clientes, gestión de pedidos, inventario y etiquetado de productos.

Tabla 2.5. Computadoras de escritorio por áreas

Área	Cantidad	Características
Gerencia General	1	MARCA: LENOVO PROCESADOR: Core i3 CPU: 3.5 GHz SISTEMA OPERATIVO: Windows 7
Área Administrativa	2	MARCA: PRODESK 400 G3 PROCESADOR: Core i5 CPU: 3.2 GHz SISTEMA OPERATIVO: Windows 10 PRO
	1	MARCA: LENOVO PROCESADOR: Core i3 CPU: 3.6 GHz SISTEMA OPERATIVO: Windows 10 PRO
Área de Producción de Cuero	1	MARCA: NIUTEK PROCESADOR: Core i3 CPU: 3.3 GHz SISTEMA OPERATIVO: Windows 10 PRO
	1	MARCA: HP PROCESADOR: Core i3 CPU: 3.2 GHz SISTEMA OPERATIVO: Windows XP
Área de Ventas	2	MARCA: HP PROCESADOR: Core i3 CPU: 3.3 GHz SISTEMA OPERATIVO: Windows 10 PRO
	1	MARCA: LENOVO PROCESADOR: Core i3 CPU: 3.5 GHz SISTEMA OPERATIVO: Windows 7

2.1.3.2.6. Computadoras Portátiles

La empresa cuenta con cuatro computadoras portátiles, en las que sus características varían según las necesidades de cada actividad.

En la **Tabla 2.6** se indican las especificaciones técnicas y las áreas a las cuales han sido asignadas.

En el Área de Tecnologías de la Información, existen dos computadoras portátiles, una de las cuales se encuentra en la Sub-área de Desarrollo Web que permite la administración y mantenimiento de la página web y botón de pagos, alimentación al inventario y edición mediante *scripts*. La otra computadora portátil está en el Área de Soporte Intranet y Software, a través de ésta se administra toda la intranet, servidor físico y virtuales, *token* digital y bases de datos confidenciales.

Para el Área de Marketing y Publicidad están designados dos computadores portátiles, que permitirán desarrollar varias funciones como: edición de fotografías, creación de contenido, elaboración de *banners* publicitarios y ejecución del plan de *marketing* digital.

Tabla 2.6. Laptops por áreas

ÁREA	CANTIDAD	CARACTERÍSTICAS
Área de Tecnologías de la Información	1	MARCA: ASUSTeK PROCESADOR: Core i7 CPU: 2.0 GHz SISTEMA OPERATIVO: Windows 7 Home SISTEMA OPERATIVO EXTRA: Linux- Debian 10
	1	MARCA: Razer Inc. PROCESADOR: Core i7 CPU: 1.3 GHz SISTEMA OPERATIVO: Windows 10 Home
Área de Marketing y Publicidad	2	MARCA: DELL PROCESADOR: Core i5 CPU: 1.8 GHz SISTEMA OPERATIVO: Windows 10 PRO

2.1.3.2.7. Sistema de videovigilancia

La empresa cuenta con un sistema de videovigilancia compuesto por 24 cámaras IP distribuidas estratégicamente en todas las áreas de la empresa, tal como se indica en la **Tabla 2.7.**

Tabla 2.7. Distribución de Cámaras IP

ÁREA	CANTIDAD	EQUIPO
Área de Tecnologías de la Información	1	Cámaras IP
Área de Ventas	6	Cámaras IP
Área Administrativa	2	Cámaras IP
Área de Producción del Cuero	10	Cámaras IP
Área de producción de Calzado y Accesorios	5	Cámaras IP

Además, cuenta con un grabador de video digital marca Hikvision (ver **Figura 2.8**), el cual permite la grabación y almacenamiento de video.

Figura 2.8. Características del DVR/NVR [31]

Las características de este dispositivo de muestran en la **Tabla 2.8.**

Tabla 2.8. Características del DVR/NVR

CARACTERÍSTICAS DEL EQUIPO	
MARCA:	Hikvision
MODELO:	*DVR/NVR DS-7216HQHI-F2/N*
TECNOLOGIAS:	AHD, HD-TVI
CANALES:	ANALÓGICO: 16CH IP: 2CH

2.1.3.2.8. Red Telefónica

Los teléfonos fijos son dispositivos de comunicación que utilizan una línea telefónica de un proveedor externo. La empresa cuenta con tres teléfonos fijos que se conectan con la central telefónica y están distribuidos en el Área Administrativa y en el Área de Ventas.

2.1.3.2.9. Telefonía Móvil

Son dispositivos móviles que tienen varias funcionalidades como: almacenar todo tipo de información, tomar fotografías, grabar videos y audios, así como conectarse a una red inalámbrica para el envío de información a través de Internet.

En la empresa se utilizan 6 dispositivos móviles en el Área de ventas que permiten fácil y rápida interacción con los clientes a nivel nacional e internacional, 2 en el Área Administrativa y 4 en el Área de Producción.

2.1.3.2.10. Impresoras

Son periféricos de salida de un computador que permiten la impresión y escaneo de documentación con texto e imágenes.

La empresa cuenta con dos impresoras multifunción que permiten la impresión y escaneo de documentos, cuatro matriciales que sirven únicamente para impresión de documentos y dos de etiquetas de código de barras. Su distribución se indica en la **Tabla 2.9.**

Tabla 2.9. Impresoras por áreas

Área	Cantidad	Equipo	Características
Área Administrativa	1	IMPRESORA MULTIFUNCIÓN	MARCA: EPSON MODELO: WF-3620
	2	IMPRESORA MATRICIAL	MARCA: EPSON MODELO: LX-300+II
Área de Producción de Cuero	1	IMPRESORA ZEBRA	MARCA: TSC MODELO: TSC-200
	1	IMPRESORA MATRICIAL	MARCA: EPSON MODELO: LX-300+II
Área de Ventas	1	IMPRESORA ZEBRA	MARCA: TSC MODELO: TSC-200
	1	IMPRESORA MATRICIAL	MARCA: EPSON MODELO: LX-300+II
	1	IMPRESORA MULTIFUNCIÓN	MARCA: EPSON MODELO: WF-3620

2.1.3.2.11. Token digital

Es una contraseña digital segura de seis dígitos que se genera en un dispositivo móvil de forma aleatoria y típicamente se renueva cada sesenta segundos, en respuesta a una solicitud de acceso o permiso de operación en servicio banca web o banca por Internet. Es utilizado para brindar mayor seguridad y facilidad en operaciones bancarias por Internet permitiendo un mecanismo de autenticación y validación sencillo [32].

La empresa posee un *token* digital para cumplir con todos los movimientos bancarios y firma digital con el Banco Central del Ecuador de una forma segura y sencilla.

2.1.3.3. Software

2.1.3.3.1. Servidor DNS

Un servidor DNS es un sistema distribuido, escalable y jerárquico de nombres de dominio, que tiene como función la traducción de nombres a direcciones IP y viceversa. Básicamente es similar a una agenda telefónica con la diferencia de que, en lugar de traducir nombres a números telefónicos, éste traduce direcciones web a direcciones IP [33].

La empresa cuenta con este servidor para la traducción de dominios internos y de los servidores virtualizados.

2.1.3.3.2. Servidor de Base de Datos Oracle XE 18c

Un servidor de base de datos es un sistema utilizado para registrar y almacenar todo tipo de datos, de tal manera que se puedan utilizar para procesos posteriores [33]. La empresa

utiliza una base de datos relacional que organiza la información y datos a través de tablas; el lenguaje de acceso a la base es SQL[11].

SQL es un lenguaje que permite consultar, actualizar, modificar, crear datos en volumen; es decir, que permite gestionar hasta millones de celdas de una tabla de datos. Para la administración y gestión de dicha base de datos se utiliza Oracle Express Edition 18c.

Es un sistema de gestión de base de datos gratuito, compatible con lenguajes de programación como PHP[12], JAVA[13] o .NET[14] [34].

Posee varias características como:

- Permite el análisis en tiempo real, debido a que almacena los datos en *Database In-Memory*[15].
- Compresión de datos avanzada, permitiendo la optimización de espacio de almacenamiento, y la mejora del rendimiento en la lectura de datos.
- Análisis avanzado de la información con predicciones a partir de los datos a través de *Data Mining* SQL[16].
- Seguridad avanzada en la protección de datos confidenciales.

La empresa hace uso de este servidor para la administración y gestión de la base de datos del sistema contable SACI (Sistema Administrativo Contable Integrado.). Dicha base de datos contiene información:

- Personal de los clientes.
- Relacionada a los proveedores.
- De estados de cuenta de clientes y proveedores de servicios.
- De balances financieros.
- De control de acceso de usuarios del sistema.

[11] SQL: *Structured Query Language*/Lenguaje de Consulta Estructurado que se utiliza para administrar bases de datos relacionales.
[12] PHP: *Hypertext Preprocessor* es un lenguaje de código abierto adecuado para el desarrollo web y que puede ser usado en HTML.
[13] JAVA: Lenguaje de programación orientado a objetos.
[14] .NET: Es un *framework* de Microsoft.
[15] *Database In-Memory*: Es un tipo de base de datos con algoritmos de última generación para los procesos en memoria y está diseñada para lograr un tiempo de respuesta mínimo.
[16] *Data Mining SQL*: Es una función de minería de datos en SQL para la predicción de datos.

- Del recurso humano.
- De datos bancarios.
- De productos terminados e inventario.
- De Kardex de productos químicos.
- De fichas de costo.

2.1.3.3.3. Servidor de Base de Datos MySQL 8.0

Es un sistema de gestión de base de datos relacional de código abierto, flexible, escalable y confiable. Además, posee una interfaz gráfica que brinda mayor facilidad de uso [35].

Algunas de las características principales son:

- Es multiproceso debido al uso de varias CPU.
- Archiva los datos en tablas separadas, lo que brinda mayor velocidad y flexibilidad.
- Tiene un sistema muy rápido de asignación de memoria basado en subprocesos.
- Es un servidor con un diseño en varias capas con módulos independientes.

La empresa implementó el servidor MySQL para la gestión de base de datos de facturación electrónica, debido a necesidad de emitir comprobantes electrónicos debidamente autorizados por el SRI como se establece en la Resolución NAC-DGERCGC13-00236, Registro Oficial 956 del 17 de mayo de 2013.

La información que almacena este servidor está relacionada a la Facturación Electrónica:

- Información de clientes.
- Información de productos terminados.
- Información de materia prima.
- Información de costos.
- *Token* Digital.
- Información de facturas, guías de remisión, notas de crédito y notas de débito.

2.1.3.3.4. Servidor de Base de Datos PostgreSQL 13

Es un sistema de base de datos relacional orientado a objetos de código abierto y gratuito, que utiliza lenguaje SQL [36].

Entre sus principales características se tienen:

- Es escalable, porque puede administrar grandes volúmenes de datos y usuarios simultáneos.
- Es un sistema con alta concurrencia; mediante el sistema MVCC[17] se puede acceder a varias tablas de manera simultánea.

La empresa implementó este servidor para la administración y gestión de la base de datos del Área de Recursos Humanos. Entre la información más relevante se tiene:

- Información personal del recurso humano.
- Información de credenciales de acceso.
- Información de contratos de trabajo.
- Información de avisos de entrada, actas de finiquito y liquidaciones de los empleados.
- Información y documentación del IESS (Instituto Ecuatoriano de Seguridad Social).

2.1.3.3.5. Servidor OwnCloud

Este servidor es un software de colaboración de contenidos, sincronización y compartición de archivos en tiempo real; realiza el cifrado de archivos y se puede trabajar desde cualquier dispositivo [37]. El acceso a sus archivos es a través de una interfaz web o WebDAV[18]. WebDAV es un protocolo de transferencia de archivos cuyo objetivo es hacer de www (*World Wide Web*/ Red Informática Mundial) un medio legible y editable [37].

OwnCloud presenta varias características:

- Permite la administración de usuarios a través del control de acceso con permisos.
- Admite la clasificación y visualización de imágenes.
- Posibilita realizar un control de versiones.

[17] MVCC: Acceso Concurrente Multi versión, método de control de acceso para implementar concurrencia.
[18] WebDAV: *Web- based Distributed Authoring and Versioning*/ Autoría y Versionado Distribuidos por Web, que proporciona funcionalidades para crear, cambiar y mover documentos en un servidor remoto

- Permite la administración de contactos mediante CardDAV[19] que es un protocolo de código abierto diseñado para sincronizar la base de datos de contactos.

La empresa cuenta con este servidor para la administración y gestión de la información y datos manejados en cada uno de los CPUs de la empresa. OwnCloud está instalado en todos los equipos de trabajo de todas las áreas, con el fin de realizar el almacenamiento de toda la información en tiempo real.

Este servidor almacena:

- La información perteneciente al Area Administrativa como: registros contables, nómina, reportes de ventas, oficios, permisos de funcionamiento, cartas de autorización, registros internos de roles de pago, reportes de declaraciones del impuesto a la renta, reportes de declaraciones del impuesto al valor agregado, archivos digitales de planillas del SRI, IESS, servicios básicos.
- La información perteneciente al Área de Producción de Cuero como: registros diarios de formulaciones químicas del cuero, formularios y registros de Kardex de productos químicos controlados por el CONSEP (Consejo Nacional de Control de Sustancias Estupefacientes y Psicotrópicas).
- La información correspondiente al Área de Producción de Calzado y Accesorios como: fotografías y diseños de los productos terminados en cuero, fichas de costos de los productos terminados, patrones a escala de cada diseño de calzado, chaquetas y carteras de cuero, formatos de etiquetas INEN para cada producto, códigos de barra para la venta y distribución de los productos terminados.
- La información relacionada al Área de Marketing y Publicidad como: fotografías en formatos JPG, PNG, RAW; videos en formato MP4; diseños, portadas y *banner*s en formato AI, PSD; reportes de gestión de ventas, registros del plan de *marketin*g de la empresa, fichas técnicas de los productos.
- La información relacionada al Área de Tecnologías de la Información como: reportes de gestión de base de datos, registros de *backup.*
- La información correspondiente al Área de Ventas como: reportes diarios de ventas; facturas, notas de débito y notas de crédito en formato PDF y XML; cartas de

[19] CardDAV: Es un protocolo de código abierto diseñado para sincronizar bases de datos de contactos

autorización y guías de envío de mercadería en formato PDF y WORD; registros de ventas diarias por vendedor.

2.1.3.3.6. Servidor FTP

El protocolo FTP proporciona un servicio orientado a conexión el cual permite la transferencia de información. El servidor FTP se encarga de recibir las peticiones de los clientes y establecer la conexión a través de los puertos 20 o 21. El mayor inconveniente de este protocolo es que los datos viajan en texto plano sin ser cifrados, por lo que es susceptible a ataques *Man-in-the-Middle*. La versión segura de este protocolo es denominada SFTP (FTP sobre SSH) que permite establecer una conexión segura [38].

La empresa cuenta con este servidor para realizar la transferencia de archivos referentes a anexos tributarios correspondientes al sistema de Facturación Electrónica, además se debe contar con acceso al servidor SFTP[20] del Servicio de Rentas Internas, para solicitar la autorización de los documentos electrónicos que deberán contener la firma electrónica correspondiente.

2.1.3.3.7. Servidor NGINX

Es un servidor web de código abierto, que dentro de sus funcionalidades están actuar como proxy inverso, balanceador de carga y proporcionar servicios de correo electrónico (IMAP, POP). Una de las principales ventajas de Nginx es el modo asíncrono, el cual le permite gestionar varias solicitudes de conexiones con pocos hilos, reduciendo el nivel de procesamiento y optimizando recursos [39].

La empresa utiliza este servidor web para interactuar con la página web y correo electrónico, debido a que brinda un alto nivel en velocidad de respuesta.

2.1.3.3.8. Servidor de Aplicaciones DigitalOcean

La empresa utiliza el plan básico que incluye un *droplet* de un CPU y 2 GB de memoria y un *droplet* de *backup.* Se hace uso de este servicio para alojar el sitio web con el siguiente dominio: www.curtiembrequisapincha.com. La administración de este sitio web se realiza a través de la plataforma WordPress.

2.1.3.3.9. Repositorio de Almacenamiento Google Drive

La empresa tiene contratado el plan Google One que brinda 100 GB de espacio de almacenamiento. La información almacenada en Google Drive está relacionada a: *backup*

[20] SFTP: Es el protocolo FTP con una capa de seguridad SSL/TLS ()

de aplicaciones de todos los dispositivos móviles de la empresa, registros de las agendas de contactos; fotografías de productos; el contenido, imágenes, videos, documentos de los correos electrónicos de *Gmail*; recursos compartidos con el equipo de trabajo del área de *marketing* y publicidad.

2.1.3.3.10. Software Contable SACI

Un software contable es un sistema informático que gestiona y registra en una base de datos todo tipo de información relacionada al giro de negocio de la empresa (ver **Figura 2.9**).

Figura 2.9. SACI – Sistema Contable

La empresa cuenta con el sistema contable SACI (Software Administrativo Contable Integral) que permite sincronizar la información relacionada a todas los procesos y actividades de la empresa [40].

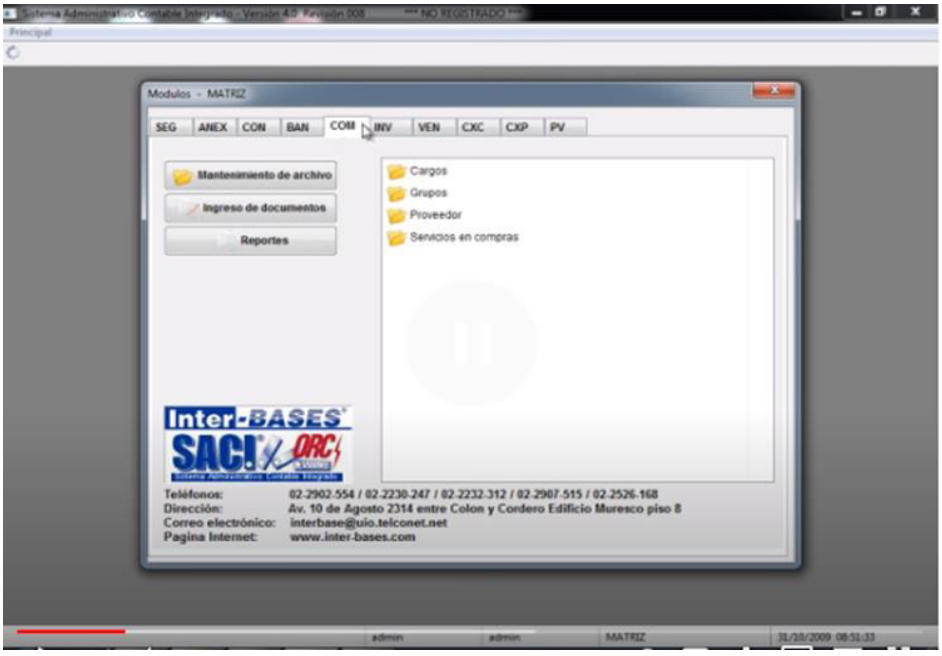


Figura 2.10. Interfaz de SACI

En la **Figura 2.10** se muestra la interfaz con todos los módulos del sistema contable. Algunos módulos importantes para el giro de negocio de la empresa son:

- **Seguridad del sistema:** En este módulo se gestiona toda la información de control de acceso de usuario y mantenimiento del sistema.
- **Contabilidad:** Este módulo presenta los balances contables y estados de cuenta de la empresa.
- **Bancos:** En este módulo se gestiona todo tipo de información referente a cartera de cheques de terceros, cheques personales y cuentas bancarias de la empresa; también gestiona los cierres de caja diarios, semanales y mensuales.
- **Compras:** Este módulo gestiona la información referente a proveedores de productos químicos, materia prima, mano de obra y servicios externos. Gestiona las facturas y retenciones correspondientes a cada compra realizada, registros de anticipos y pagos de servicios.
- **Inventarios:** En este módulo se gestionan los productos terminados y materia prima que posee la empresa, al igual que los productos utilizados en procesos intermedios. También la información relacionada a listas de precios, hojas de costos de cada producto y reportes de mercadería existente en *stock*.
- **Ventas:** Este módulo gestiona la información de clientes, facturación electrónica, notas de crédito y notas de débito correspondientes a la venta de mercadería y productos terminados. También permite generar reportes de ventas diarias, semanales y mensuales según varios filtros de datos.
- **Cuentas por cobrar:** Este módulo gestiona la cartera de clientes potenciales de la empresa, así como la información relacionada a estados de cuenta de clientes, anticipos, abonos, registros de cheques, depósitos e ingresos de la empresa.
- **Cuentas por pagar:** Este módulo gestiona la cartera de proveedores de la empresa, al igual que la información relacionada a estados de cuenta de proveedores, registros de pagos y control de anticipos y egresos de la empresa.

2.1.3.3.11. Sitio Web

Es un conjunto de páginas web sujetas a un dominio y alojadas en un servidor web para su funcionamiento.

La empresa cuenta con un sitio web con la URL www.curtiembrequisapincha.com como se muestra en la **Figura 2.11**, que está alojada en los servidores virtuales de Digital Ocean. Cuenta con un certificado SSL y un botón de pagos de Paymentez.

Figura 2.11. Sitio Web de la empresa [21]

2.1.4. ESTADO DE SITUACIÓN ACTUAL DE LA SEGURIDAD DE LA INFORMACIÓN DE LA ORGANIZACIÓN

El Área Tecnologías de la Información de la empresa fue implementada con el objetivo de crecer en el mercado virtual a nivel mundial; para esto se ha implementado una tienda virtual *E-commerce* en la plataforma WordPress, lo que ha permitido posesionar a la empresa en las redes sociales con más auge.

Para obtener una visión general de la seguridad de la información de la empresa, se ha entrevistado al jefe del Área de Tecnologías de la Información, con el tema: "Identificación de brechas, incidentes y riesgos existentes en la seguridad de la información de la empresa", como se muestra en el **ANEXO A** de este proyecto.

En base a la entrevista se pudo identificar la siguiente información:

- Existen incidentes de seguridad de la información registrados, que causaron la filtración de datos del Área de Administración, los mismos que han perjudicado a los ingresos económicos de la empresa.
- Existen brechas de seguridad de la información, debido a que no se tiene establecido un proceso de control de acceso en los equipos de la empresa.
- No se realiza campañas de concientización, al interior de la empresa, en temas de seguridad de la información.
- Existen roles de usuarios definidos para el acceso del sistema contable, pero no existen roles para el acceso a los sistemas operativos de los computadores.

- No existe un servicio de respaldo para subsanar la falta del servicio de Internet, el mismo que es un servicio crítico externo que la empresa utiliza para el giro de negocio.
- No existen políticas, controles, ni procedimientos establecidos para la gestión de la seguridad de la información.
- El mayor riesgo existente en la empresa es la filtración de datos y fuga de información referente a la parte administrativa de la empresa.

En base a la entrevista realizada se puede identificar la falta de un diseño e implementación de un Sistema de Gestión de Seguridad de la Información, debido a que la empresa no gestiona la seguridad de la información en función de normas y buenas prácticas de seguridades. La falta de gestión ha ocasionado incidentes de seguridad como filtración y fuga de información confidencial de la empresa.

La gestión de riesgos de seguridad de la información y la identificación de brechas existentes en los activos de la empresa, se la realizará de forma detallada en la etapa de diseño del SGSI.

2.1.5. DEFINICIÓN DEL ALCANCE DEL SGSI

El presente proyecto de titulación plantea realizar el diseño del Sistema de Gestión de la Seguridad de la Información (SGSI) para la empresa Curtiembre Quisapincha ubicada en la provincia de Tungurahua.

El SGSI tiene un enfoque en función del giro de negocio de la empresa y sus necesidades; el mismo estará basado en la infraestructura tecnológica y la información confidencial de la empresa.

El alcance del SGSI cubre la fase de planeación que permitirá la identificación y valoración de activos, amenazas, impacto y riesgo de cada activo, teniendo como objetivo definir un plan de políticas y procedimientos de seguridad de la información. El desarrollo se llevará a cabo en función de la metodología MAGERIT v3.0 y la Norma Técnica Ecuatoriana ISO27001:2013.

2.1.6. DEFINICIÓN DE LOS LÍMITES DEL SGSI

En el diseño del SGSI no se incluirán las siguientes cláusulas mandatorias: soporte, operación, evaluación de desempeño y mejora del sistema. Así también, en el análisis no se considerará la gestión de recursos humanos, proveedores externos y la infraestructura física de las instalaciones de la empresa, elementos que están fuera del alcance del SGSI.

2.1.7. ESTABLECIMIENTO DEL SGSI

El establecimiento del Sistema de Gestión de Seguridad de la Información (SGSI) tiene como objetivo identificar las amenazas que pueden afectar directamente a los activos de la infraestructura tecnológica de la empresa. A partir de dicha identificación se determinarán las amenazas, el impacto que generaría la materialización de estas sobre los activos y los riesgos, con el fin de realizar el tratamiento del riesgo.

2.2. LIDERAZGO

Los puntos para tratar en esta cláusula son liderazgo y compromiso y política de seguridad.

2.2.1. LIDERAZGO Y COMPROMISO

El liderazgo y compromiso de la alta dirección es indispensable en el desarrollo del Sistema de Gestión de Seguridad de la Información, debido a que para el diseño del SGSI de Curtiembre Quisapincha, la Alta Dirección debe cumplir con las siguientes funciones:

- Garantizar el cumplimiento de la política de seguridad de la información.
- Brindar facilidad de accesos a los recursos e información necesaria.
- Realizar capacitaciones al personal de la empresa.
- Definir roles y responsabilidades.

2.2.2. POLÍTICA DE SEGURIDAD

La alta dirección debe establecer una política de seguridad de la información, apropiada al giro de negocio de la organización, incluir los objetivos de seguridad de la información y el compromiso de cumplir con las condiciones que se pueden aplicar referente a la seguridad de la información. Además, la política debe estar documentada, notificada a las partes interesadas y concientizada al personal de la organización [14]. La política de seguridad de la información de Curtiembre Quisapincha se la desarrollará en el Capítulo 3 correspondiente a resultados y discusión.

2.3. PLANIFICACIÓN

La cláusula de planificación hace referencia a la metodología, análisis y gestión de los riesgos del sistema de seguridad de la información, donde se deben establecer los criterios de valoración antes de aplicar la metodología propuesta.

2.3.1. CRITERIOS DE VALORACIÓN

Para el diseño del Sistema de Gestión de Seguridad de la Información se han establecido varios pasos a seguir en función de la metodología MAGERIT [10] y la norma ISO 27001:2013 [14]**.** Así también, se deben establecer modelos de valoración o estimación, por lo que se considera la valoración cualitativa y la valoración cuantitativa como pilares para poder realizar este análisis.

- **Valoración cualitativa**

La valoración cualitativa brinda mayor facilidad en el entendimiento, porque hace referencia a una escala de atributos calificativos para describir las características y dimensiones de un activo [18].

- **Valoración cuantitativa**

La valoración cuantitativa utiliza una escala numérica que brinda mayor precisión en los valores y busca cuantificar todos los aspectos posibles de un activo [18].

2.3.1.1. Criterios de valoración de los Activos de Información

El valor del activo se compone del costo del activo y el costo por dimensiones [17], para obtener el costo del activo se utilizará la valoración cuantitativa que permitirá el uso de escalas numéricas que brindan mayor precisión que la valoración cualitativa. Mientras que, para obtener el costo en cada dimensión de seguridad, se utilizará la valoración cualitativa, para determinar el costo que supondría el fallo o pérdida de dichas dimensiones en cada activo.

2.3.1.1.1. Costo del activo

El costo del activo se refiere al costo original, de reposición o renovación de un activo y al daño o pérdidas económicas que ocasionaría en la empresa [17].

- ***Costo original del activo***

Se refiere al costo o valor económico del activo. La escala de valoración del costo del activo que se muestra en la **Tabla 2.10**, establece niveles del 1 al 5, donde el valor 1 representa a un nivel muy bajo o de costo mínimo y el valor 5 representa a un nivel muy alto o de costo alto.

Esta escala de valoración fue planteada en función de la siguiente pregunta:

¿Si existe destrucción del activo, cuál es el nivel de afectación al costo original del activo?

Tabla 2.10. Escala de valoración del costo original del activo

[COS] COSTO ORIGINAL DEL ACTIVO		
VALOR	**NIVEL**	**COSTO ORIGINAL**
1	Muy bajo	El costo del original del activo es muy bajo.
2	Bajo	El costo del original del activo es bajo.
3	Moderado	El costo del original del activo es moderado.
4	Alto	El costo del activo es alto.
5	Muy alto	El costo del activo es muy alto.

- ***Daño económico a la empresa***

Se refiere a las pérdidas económicas que se generarían en la empresa a causa de la destrucción del activo.

La escala de valoración del daño económico a la empresa que se muestra en la **Tabla 2.11**, establece niveles del 1 al 5, donde el valor 1 representa un nivel muy bajo o de pérdidas mínimas y el valor 5 representa un nivel muy alto o de pérdidas graves.

Esta escala de valoración fue planteada en función de la siguiente pregunta:

¿Si existe destrucción del activo, se generan pérdidas económicas en la empresa?

Tabla 2.11. Daño económico a la empresa

[DE] DAÑO ECONÓMICO/ LUCRO SESANTE		
VALOR	**NIVEL**	**DAÑO ECONÓMICO**
1	Muy bajo	No genera pérdidas económicas en la empresa.
2	Bajo	Genera pérdidas económicas mínimas en la empresa.
3	Moderado	Genera pérdidas económicas considerables en la empresa.
4	Alto	Genera pérdidas económicas muy elevadas en la empresa.
5	Muy alto	Genera pérdidas económicas graves en la empresa.

- ***Resultado del costo del activo***

El costo del activo se lo calcula en función al nivel de afectación que implica el costo original del activo y el daño económico que ocasiona a la empresa, como indica la Ecuación 2.1.

$$[C_A] = [C_{o,r}] + [D_E] \quad (2.1)$$

Donde,

$[C_A]$: Costo del activo

$[C_{o,r}]$: Costo original, reposición

$[D_E]$: Daño económico a la empresa

El costo del activo será reducido a una escala normal del 1 al 5 a partir de una escala extendida de 10 valores como se indica en la **Tabla 2.12**, debido a que se toman en cuenta dos criterios importantes para el análisis.

Tabla 2.12. Costo del Activo

COSTO DEL ACTIVO			
ESCALA EXTENDIDA	**ESCALA**	**NIVEL DE AFECTACION**	**DESCRIPCIÓN**
1-2	1	Insignificante	El costo del activo es insignificante, si existe destrucción del activo.
3-4	2	Poco Importante	El costo del activo es poco importante, si existe destrucción del activo.
5-6	3	Importante	El costo del activo es importante, si existe destrucción del activo.
7-8	4	Muy importante	El costo del activo es muy importante, si existe destrucción del activo.
9-10	5	Crítico	El costo del activo es crítico, si existe destrucción del activo.

2.3.1.1.2. Costo por dimensiones

El costo por dimensiones se lo obtiene a partir de la suma del costo en las dimensiones de Integridad, Confidencialidad y Disponibilidad. Estos costos serán obtenidos en función de criterios de las posibles consecuencias debido a la pérdida de Integridad, Confidencialidad y Disponibilidad de un activo.

Los criterios de consecuencias para evaluar cada dimensión se los seleccionó a partir de las escalas estándar que se especifican en el Libro II de la metodología MAGERIT v.3 [11] y se los detalla a continuación:

a. [si] Seguridad

b. [cei] Intereses comerciales o económicos

c. [da] Interrupción del servicio

d. [adm] Administración y gestión

e. [lg] Pérdida de confianza (reputación)

f. [rto] Tiempo de recuperación del servicio

A continuación, se detallan las escalas de valoración de cada criterio para evaluar las consecuencias generadas a causa de la pérdida de las dimensiones de seguridad en un activo. Además, se establecen niveles del 1 al 5, donde el valor 1 representa a un nivel muy bajo o un valor de afectación nulo, mínimo o insignificante y el valor 5 representa a un nivel muy alto o un valor de afectación grave, fatal o catastrófico.

a. [si] Seguridad

Se refiere a la seguridad de la información de los activos de la empresa. Las dimensiones implicadas en este criterio son: Integridad, Confidencialidad o Disponibilidad.

La escala de valoración que se indica en la **Tabla 2.13** fue planteada en función de la siguiente pregunta:

¿Si existe pérdida de Integridad, Confidencialidad o Disponibilidad en un activo, la seguridad de la información se ve afectada?

Tabla 2.13. Escala de valoración para la seguridad [si]

[si] SEGURIDAD		
ESCALA	**NIVEL**	**DESCRIPCIÓN**
1	Muy bajo	La pérdida de Integridad, Confidencialidad o Disponibilidad del activo puede causar fallos en la seguridad de la información.
2	Bajo	La pérdida de Integridad, Confidencialidad o Disponibilidad del activo probablemente cause fallos en la seguridad de la información.
3	Moderado	La pérdida de Integridad, Confidencialidad o Disponibilidad del activo probablemente sea causa de un incidente de seguridad de la información.
4	Alto	La pérdida de Integridad, Confidencialidad o Disponibilidad del activo probablemente sea causa de un grave incidente de seguridad de la información.
5	Muy alto	La pérdida de Integridad, Confidencialidad o Disponibilidad del activo probablemente sea causa de un incidente muy grave de seguridad de información.

b. *[cei] Intereses comerciales o económicos*

Se refiere a la importancia de la afectación económica de un activo y consecuentemente las posibles pérdidas económicas a la empresa; así también al grado de interés que se genera en las empresas que son competencia directa. Este criterio afecta a las dimensiones de Integridad, Confidencialidad o Disponibilidad.

La escala de valoración que se indica en la **Tabla 2.14** fue planteada en función de la siguiente pregunta:

¿Si existe pérdida de Integridad, Confidencialidad o Disponibilidad en un activo, los intereses comerciales y económicos de la empresa se ven afectados?

Tabla 2.14. Escala de valoración para los intereses comerciales o económicos [cei]

[cei] INTERESES COMERCIALES O ECONÓMICOS		
ESCALA	**NIVEL**	**DESCRIPCIÓN**
1	Muy bajo	La pérdida de Integridad, Confidencialidad o Disponibilidad del activo es causa de pérdidas económicas mínimas en la empresa y sin interés para la competencia.
2	Bajo	La pérdida de Integridad, Confidencialidad o Disponibilidad es causa de pérdidas económicas bajas en la empresa y un bajo interés para la competencia.
3	Moderado	La pérdida de Integridad, Confidencialidad o Disponibilidad es causa de pérdidas económicas significativas en la empresa e interés para la competencia.
4	Alto	La pérdida de Integridad, Confidencialidad o Disponibilidad es causa de pérdidas económicas graves en la empresa y un alto interés para la competencia.
5	Muy alto	La pérdida de Integridad, Confidencialidad o Disponibilidad es causa de pérdidas económicas fatales en la empresa y de gran interés para la competencia.

c. *[da] Interrupción del servicio*

Se refiere a la interrupción de las actividades o servicios que afectan directamente a los activos de la empresa. La dimensión implicada en este criterio es Disponibilidad.

La escala de valoración que se indica en la

Tabla 2.15 fue planteada en función de la siguiente pregunta:

¿Si existe pérdida de Disponibilidad en un activo, se genera interrupción de las actividades de la empresa?

Tabla 2.15. Escala de valoración para la interrupción del servicio [da]

[da] INTERRUPCIÓN DEL SERVICIO		
ESCALA	**NIVEL**	**DESCRIPCIÓN**
1	Muy bajo	La pérdida de Disponibilidad del activo probablemente no interrumpa a ninguna actividad de la empresa.
2	Bajo	La pérdida de Disponibilidad del activo probablemente no cause interrupción de las actividades de la empresa.
3	Moderado	La pérdida de Disponibilidad del activo probablemente interrumpa pocas actividades de la empresa.
4	Alto	La pérdida de Disponibilidad del activo probablemente interrumpa algunas actividades de la empresa.
5	Muy alto	La pérdida de Disponibilidad del activo probablemente cause una interrupción grave en todas las actividades de la empresa.

d. [adm] Administración y gestión

Se refiere al nivel de operación efectiva de la empresa [11]. Las dimensiones implicadas en este criterio son: Integridad, Confidencialidad o Disponibilidad.

La escala de valoración **Tabla 2.16** fue planteada en función de la siguiente pregunta:

¿Si existe pérdida de Integridad, Confidencialidad o Disponibilidad en un activo, la administración y gestión de la empresa se ve afectada?

Tabla 2.16. Escala de valoración de la administración y gestión [adm]

[adm] ADMINISTRACIÓN Y GESTIÓN		
ESCALA	**NIVEL**	**DESCRIPCIÓN**
1	Muy bajo	La pérdida de Integridad, Confidencialidad o Disponibilidad del activo pudiera impedir la operación efectiva de una parte de la empresa.
2	Bajo	La pérdida de Integridad, Confidencialidad o Disponibilidad del activo probablemente impediría la operación efectiva de una parte de la empresa.
3	Moderado	La pérdida de Integridad, Confidencialidad o Disponibilidad del activo probablemente impediría la operación efectiva de más de una parte de la empresa.
4	Alto	La pérdida de Integridad, Confidencialidad o Disponibilidad del activo probablemente impediría la operación efectiva de la empresa.
5	Muy alto	La pérdida de Integridad, Confidencialidad o Disponibilidad del activo probablemente impediría seriamente la operación efectiva de la empresa, pudiendo llegar a su paralización.

e. *[lg] Pérdida de confianza (reputación)*

Se refiere a la pérdida de confianza del cliente, pérdida de credibilidad en el sistema de información y daño en la reputación de la imagen de la empresa [17]. Las dimensiones implicadas en este criterio son: Integridad, Confidencialidad o Disponibilidad.

La escala de valoración que se indica en la **Tabla 2.17** fue planteada en función de la siguiente pregunta:

¿Si existe pérdida de Integridad, Confidencialidad o Disponibilidad en un activo, la confianza del cliente y reputación de la imagen de la empresa se ve afectada?

Tabla 2.17. Escala de valoración para la pérdida de confianza(reputación) [lg]

[lg] PÉRDIDA DE CONFIANZA (REPUTACIÓN)		
ESCALA	**NIVEL**	**DESCRIPCIÓN**
1	Muy bajo	La pérdida de Integridad, Confidencialidad o Disponibilidad del activo no supondría daño a la confianza, reputación o buena imagen de las personas o de la empresa.
2	Bajo	La pérdida de Integridad, Confidencialidad o Disponibilidad del activo probablemente cause una pérdida menor de confianza, reputación o buena imagen de las personas o de la empresa.
3	Moderado	La pérdida de Integridad, Confidencialidad o Disponibilidad del activo probablemente sea causa de cierta publicidad negativa por afectar negativamente a las personas o a las relaciones con otras empresas.
4	Alto	La pérdida de Integridad, Confidencialidad o Disponibilidad del activo probablemente causaría una publicidad negativa por afectar gravemente a las personas o a las relaciones con otras empresas.
5	Muy alto	La pérdida de Integridad, Confidencialidad o Disponibilidad del activo probablemente sea causa de una publicidad negativa por afectar de forma fatal a las personas o a las relaciones con otras empresas.

f. *[rto] Tiempo de recuperación del servicio*

Se refiere al tiempo que se tarda en el restablecimiento o recuperación de un activo fallido. Este criterio afecta a las dimensiones de Confidencialidad y Disponibilidad.

La escala de valoración que se indica en la **Tabla 2.18** fue planteada en función de la siguiente pregunta:

¿Si existe pérdida de Confidencialidad o Disponibilidad en un activo, cuál será el tiempo de recuperación del servicio?

Tabla 2.18. Escala de valoración para el tiempo de recuperación del servicio (RTO)

[rto] TIEMPO DE RECUPERACIÓN DEL SERVICIO		
ESCALA	**NIVEL**	**DESCRIPCIÓN**
1	Muy bajo	La pérdida de Confidencialidad o Disponibilidad del activo pudiera causar un RTO (Recovery Time Objetive) mayor a 5 días que la empresa puede soportar sin aplicaciones o servicios, lo mismo que generaría una baja o nula afectación a las actividades de la empresa.
2	Bajo	La pérdida de Confidencialidad o Disponibilidad del activo pudiera causar un RTO menor a 5 días y mayor que 1 día, tiempo que la empresa puede soportar sin aplicaciones o servicios, lo mismo que generaría una mínima afectación a las actividades de la empresa.
3	Moderado	La pérdida de Confidencialidad o Disponibilidad del activo pudiera causar un RTO menor a 1 día y mayor que 4 horas, tiempo que la empresa puede soportar sin aplicaciones o servicios, lo mismo que generaría afectación moderada a las actividades de la empresa.
4	Alto	La pérdida de Confidencialidad o Disponibilidad del activo pudiera causar un RTO menor a 4 horas y mayor que 2 horas, tiempo que la empresa puede soportar sin aplicaciones o servicios, lo mismo que generaría una grave afectación a las actividades de la empresa.
5	Muy alto	La pérdida de Confidencialidad o Disponibilidad del activo pudiera causar un RTO menor a 2 horas, tiempo que la empresa puede soportar sin aplicaciones o servicios, lo mismo que generaría una grave afectación y pérdidas económicas a la empresa.

Una vez establecidas las escalas de valoración para cada criterio de consecuencia, se realiza un breve análisis para determinar los criterios relacionados a cada dimensión como se muestra en la **Tabla 2.19** y se obtiene las ecuaciones que indican la suma de dichos criterios correspondientes a cada dimensión como se indica en las ecuaciones 2.2, 2.3 y 2,4.

Tabla 2.19. Dimensiones de seguridad con los criterios de consecuencias

	[i] Integridad	**[c] Confidencialidad**	**[d] Disponibilidad**
[si] Seguridad	X	X	X
[cei] Intereses comerciales o económicos	X	X	X
[da] Interrupción del servicio			X
[adm] Administración y gestión	X	X	X
[lg] Pérdida de confianza (reputación)	X	X	X
[rto] Tiempo de recuperación del servicio		X	X

- ***Ecuación 2.2 referente al valor de la integridad:***

$$[i] = [si] + [cei] + [adm] + [lg] \quad (2.2)$$

- ***Ecuación 2.3 referente al valor de la confidencialidad:***

$$[c] = [si] + [cei] + [adm] + [lg] + [rto] \quad (2.3)$$

- ***Ecuación 2.4 referente al valor de la disponibilidad:***

$$[d] = [si] + [cei] + [da] + [adm] + [lg] + [rto] \quad (2.4)$$

Donde,

$[i]$: Integridad

$[c]$ Confidencialidad

$[d]$: Disponibilidad

$[si]$: Seguridad

$[cei]$: Intereses comerciales o económicos

$[da]$: Interrupción del servicio

$[adm]$: Administración y gestión

$[lg]$: Pérdida de confianza (reputación)

$[rto]$: Tiempo de recuperación del servicio

A partir de cada ecuación se obtiene el costo por cada dimensión en escala extendida, se transforma a una escala normal haciendo uso de las escalas de valoración que se muestran en las siguientes tablas:

[i] INTEGRIDAD

En la **Tabla 2.20** se establece un rango de importancia en escala extendida de 20 valores debido a que son 4 criterios relacionados con esta dimensión y se establece una escala normal de 5 valores, por efecto de resultados.

Tabla 2.20. Escala Valoración de la INTEGRIDAD

ESCALA EXTENDIDA	ESCALA NORMAL	NIVEL DE AFECTACIÓN	DESCRIPCIÓN
1-4	1	Muy bajo	La modificación de la información del activo no tendría repercusiones sobre la empresa.
5-8	2	Bajo	La modificación de la información del activo tendría repercusiones bajas sobre la empresa.
9-12	3	Moderado	La modificación de la información del activo tendría repercusiones relevantes sobre la empresa.
13-16	4	Alto	La modificación de la información del activo tendría repercusiones graves sobre la empresa.
17-20	5	Muy alto	La modificación de la información del activo tendría repercusiones fatales sobre la empresa.

[c] CONFIDENCIALIDAD

En la **Tabla 2.21** se establece un rango de importancia en escala extendida de 25 valores debido a que son 5 criterios relacionados con esta dimensión y se establece una escala normal de 5 valores, por efecto de resultados.

Tabla 2.21. Escala de valoración de la CONFIDENCIALIDAD

ESCALA EXTENDIDA	ESCALA	NIVEL DE AFECTACIÓN	CRITERIO
1-5	1	Muy bajo	La información del activo es de uso público, la divulgación no tiene afectación negativa.
6-10	2	Bajo	La información del activo es de uso limitado, la divulgación tiene afectación negativa baja.
11-15	3	Moderado	La información del activo es de uso restringido, la divulgación tiene afectación significativa.
16-20	4	Alto	La información del activo es de uso confidencial, la divulgación tiene afectación grave.
21-25	5	Muy alto	La información del activo es de uso secreto, la divulgación tiene afectación fatal.

[d] DISPONIBILIDAD

En la **Tabla 2.22** se establece un rango de importancia en escala extendida de 30 valores debido a que son 6 criterios relacionados con esta dimensión y se establece una escala normal de 5 valores, por efecto de resultados.

Tabla 2.22. Escala de valoración de la DISPONIBILIDAD

DISPONIBILIDAD			
ESCALA EXTENDIDA	**ESCALA NORMAL**	**NIVEL DE AFECTACIÓN**	**DESCRIPCIÓN**
1-6	1	Muy bajo	En el caso de indisponibilidad de la información el activo no tendría impacto sobre la empresa.
6-12	2	Bajo	En el caso de indisponibilidad de la información el activo tendría impacto bajo sobre la empresa.
13-18	3	Moderado	En el caso de indisponibilidad de la información el activo tendría impacto moderado sobre la empresa.
19-24	4	Alto	En el caso de indisponibilidad de la información el activo tendría gran impacto sobre la empresa.
25-30	5	Muy alto	En el caso de indisponibilidad de la información el activo tendría impacto total sobre la empresa.

Una vez realizada la reducción de los valores obtenidos en cada dimensión a escala normal, se obtiene el costo total por dimensiones.

- ***Resultado del costo total por dimensiones***

Para obtener el costo por dimensiones se suman los valores correspondientes a Integridad, Confidencialidad y Disponibilidad como se muestra en la Ecuación 2.5.

$$[C_{Td}] = [Vt_i] + [Vt_c] + [Vt_d] \quad (2.5)$$

Dónde,

$[C_{Td}]$: Costo total por dimensiones

$[Vt_i]$: Valor Total de Integridad

$[Vt_c]$: Valor Total de Confidencialidad

$[Vt_d]$: Valor Total de Disponibilidad

La **Tabla 2.23** indica la escala extendida de 15 valores, debido a que son 3 dimensiones de seguridad para obtener el costo total por dimensiones; además indica la escala normal del 1 al 5 que se usa en la obtención de resultado del costo total por dimensiones.

Tabla 2.23. Costo total por dimensiones

COSTO TOTAL POR DIMENSIONES			
ESCALA EXTENDIDA	**ESCALA**	**NIVEL DE AFECTACIÓN**	**DESCRIPCIÓN**
1-3	1	Insignificativo	El costo por dimensiones del activo valorado es insignificante en el caso que exista la pérdida de Integridad, Confidencialidad y Disponibilidad.
4-6	2	Poco Importante	El costo por dimensiones del activo valorado es poco importante en el caso que exista la pérdida de Integridad, Confidencialidad y Disponibilidad.
7-9	3	Importante	El costo por dimensiones del activo valorado es importante en el caso que exista la pérdida de Integridad, Confidencialidad y Disponibilidad.
10-12	4	Muy importante	El costo por dimensiones del activo valorado es muy importante en el caso que exista la pérdida de Integridad, Confidencialidad y Disponibilidad.
13-15	5	Crítico	El costo por dimensiones del activo valorado es crítico en el caso que exista la pérdida de Integridad, Confidencialidad y Disponibilidad.

2.3.1.1.3. Valor del activo

Finalmente, se obtiene el resultado del valor del activo mediante la suma del costo del activo y el costo por dimensiones, como se indica en la Ecuación 2.6.

$$[V_A] = [C_A] + [C_{Td}] \quad (2.6)$$

Donde,

$[V_A]$: Valor del activo

$[C_A]$: Costo total del activo

$[C_{Td}]$: Costo total por dimensiones

Todos los valores de los activos serán reducidos a escalas del 1 al 5 para poder realizar un análisis que sea entendible para el usuario (ver **Tabla 2.24**).

Tabla 2.24. Valor del activo

VALOR DEL ACTIVO			
ESCALA EXTENDIDA	**ESCALA NORMAL**	**VALOR**	**CRITERIO**
1-2	1	Muy bajo	El valor del activo es muy bajo y no tiene relevancia para la empresa.
3-4	2	Bajo	El valor del activo es bajo y tiene relevancia mínima en la empresa.
5-6	3	Moderado	El valor del activo es moderado y tiene un valor muy importante para la empresa.
7-8	4	Alto	El valor del activo es alto y tiene una relevancia alta en la empresa.
9-10	5	Muy alto	El valor del activo es muy alto y tiene una relevancia crítica para la empresa.

2.3.1.2. Criterios de valoración de las Amenazas

Para la valoración de las Amenazas se debe estimar la degradación del valor de los activos y la probabilidad de ocurrencia de una amenaza sobre un activo.

2.3.1.2.1. Degradación del valor por dimensiones

La degradación del valor de un activo mide el daño que puede causar un incidente en el caso de que éste ocurriera y se la puede analizar como una fracción del valor del activo; por ejemplo, un activo se ha degradado en una fracción o en su totalidad [10].

MAGERIT v.3 establece una escala cualitativa o numérica que indica una frecuencia de ocurrencia, la cual se puede apreciar en la **Tabla 2.25**.

¿Si existiera daño a un activo a causa de un incidente, cuál sería su nivel de degradación?

Tabla 2.25. Degradación del valor por dimensiones [10]

DEGRADACIÓN DEL VALOR: INTEGRIDAD, CONFIDENCIALIDAD Y DISPONIBILIDAD			
ESCALA NUMÉRICA	**NIVEL DE AFECTACIÓN**		**DESCRIPCIÓN**
1	MB	Muy bajo	Si existiera daño de un activo a causa de un incidente, es **muy raro** que le ocasione degradación de valor en las dimensiones de Integridad, Confidencialidad o Disponibilidad.
2	B	Bajo	Si existiera daño de un activo a causa de un incidente, es **poco probable** que le ocasione degradación de valor en las dimensiones de Integridad, Confidencialidad o Disponibilidad.
3	M	Moderado	Si existiera daño de un activo a causa de un incidente, es **posible** que le ocasione degradación de valor en las dimensiones de Integridad, Confidencialidad o Disponibilidad.
4	A	Alto	Si existiera daño de un activo a causa de un incidente, es **muy alta** la posibilidad de que le ocasione degradación de valor en las dimensiones de Integridad, Confidencialidad o Disponibilidad.
5	MA	Muy alto	Si existiera daño de un activo a causa de un incidente, es **casi seguro** que le ocasione degradación de valor en las dimensiones de Integridad, Confidencialidad o Disponibilidad.

- ***Escala de valoración para la degradación total***

Para obtener el valor de la degradación total se suman los valores correspondientes a la degradación de la Integridad, Confidencialidad y Disponibilidad como se muestra en la Ecuación 2.7.

$$[D_T] = [D_{v-i}] + [D_{v-c}] + [D_{v-d}] \quad (2.7)$$

Donde,

$[D_T]$: Degradación total

En la **Tabla 2.26** se muestra la escala extendida de 15 valores, que para una mejor compresión y análisis se simplifica a una escala normal comprendida entre 1 y 5.

Tabla 2.26. Degradación total

DEGRADACIÓN TOTAL				
ESCALA EXTENDIDA	**ESCALA NUMÉRICA**	**NIVEL DE AFECTACIÓN**		**DESCRIPCIÓN**
1-3	1	MB	Muy bajo	Si existiera daño de un activo a causa de un incidente, es **muy raro** que le ocasione degradación total.
4-6	2	B	Bajo	Si existiera daño de un activo a causa de un incidente, es **poco probable** que le ocasione degradación total.
7-9	3	M	Moderado	Si existiera daño de un activo a causa de un incidente, es **posible** que le ocasione degradación total.
10-12	4	A	Alto	Si existiera daño de un activo a causa de un incidente, es **muy alta** la posibilidad de que le ocasione degradación total.
13-15	5	MA	Muy alto	Si existiera daño de un activo a causa de un incidente, es **casi seguro** que le ocasione degradación total.

2.3.1.2.2. Probabilidad de ocurrencia

La probabilidad de ocurrencia mide la probabilidad de que una amenaza se materialice sobre un activo en un intervalo de tiempo.

MAGERIT v.3 establece una escala cualitativa o numérica que indica una frecuencia de ocurrencia, la cual se puede apreciar en la **Tabla 2.27**.

¿Cuál es la probabilidad de que se materialice una amenaza sobre un activo?

Tabla 2.27. Probabilidad de ocurrencia

PROBABILIDAD DE OCURRENCIA			
ESCALA NUMÉRICA	**NIVEL DE AFECTACIÓN**		**DESCRIPCIÓN**
1	MB	Muy poco frecuente	La probabilidad de que se materialice una amenaza es muy baja. Podría suceder en siglos.
2	B	Poco frecuente	La probabilidad de que se materialice una amenaza es baja. Podría suceder en varios años.
3	M	Moderado	La probabilidad de que se materialice una amenaza es normal. Podría suceder una vez al año.
4	A	Frecuente	La probabilidad de que se materialice una amenaza es frecuente. Podría suceder mensualmente
5	MA	Muy frecuente	La probabilidad de que se materialice una amenaza es muy alta. Podría suceder a diario.

2.3.1.3. Criterios de valoración del Impacto Potencial

2.3.1.3.1. Impacto Potencial por dimensiones

El impacto es la medida del daño sobre un activo, si ocurriera la materialización de una amenaza [10].

El Impacto Potencial por dimensiones es igual al nivel de degradación en cada dimensión por el valor del activo, sin tomar en cuenta los controles existentes.

- ***Ecuación 2.8 referente al Impacto Potencial en Integridad:***

$$[I_i] = [V_A]x[D_{V-i}] \quad (2.8)$$

Donde,

$[V_A]$: Valor del activo

$[I_i]$: Impacto Potencial - Integridad

$[D_{V\text{-}i}]$: Degradación de valor por Integridad

- ***Ecuación 2.9 referente al Impacto Potencial en Confidencialidad:***

$$[I_c] = [V_A]x[D_{V-c}] \quad (2.9)$$

Donde,

$[V_A]$: Valor del activo

$[I_c]$: Impacto Potencial - Confidencialidad

$[D_{V-c}]$: Degradación de valor por Confidencialidad

- ***Ecuación 2.10 referente al Impacto Potencial en Disponibilidad:***

$$[I_d] = [V_A]x[D_{V-d}] \quad (2.10)$$

Donde,

$[V_A]$: Valor del activo

$[I_d]$: Impacto Potencial - Disponibilidad

$[D_{V-d}]$: Degradación de valor por Disponibilidad

Una vez calculado el valor del Impacto Potencial por cada dimensión se hace uso de una escala extendida de 25 valores, debido a que se realiza la multiplicación de dos valores con límite 5. Los resultados se muestran en una escala normal de 5 valores, como se presenta en la **Tabla 2.28**.

. **Tabla 2.28.** Escala de valoración del Impacto Potencial por dimensiones

IMPACTO POTENCIAL POR DIMENSIONES: INTEGRIDAD, CONFIDENCIALIDAD O DISPONIBILIDAD			
ESCALA EXTENDIDA	**ESCALA NORMAL**	**IMPACTO**	**DESCRIPCIÓN**
1-5	1	Muy bajo	El Impacto Potencial de Integridad, Confiabilidad o Disponibilidad en el valor del activo es **muy bajo** y tendría relevancia **insignificativa** si ocurriera la materialización de una amenaza.
6-10	2	Bajo	El Impacto Potencial de Integridad, Confiabilidad o Disponibilidad en el valor del activo es **bajo** y tendría relevancia **leve** si ocurriera la materialización de una amenaza.
11-15	3	Moderado	El Impacto Potencial de Integridad, Confiabilidad o Disponibilidad en el valor del activo es **moderado** y tendría relevancia **significativa** si ocurriera la materialización de una amenaza.
16-20	4	Alto	El Impacto Potencial de Integridad, Confiabilidad o Disponibilidad en el valor del activo es **alto** y tendría relevancia **importante** si ocurriera la materialización de una amenaza.
21-25	5	Muy alto	El Impacto Potencial de Integridad, Confiabilidad o Disponibilidad en el valor del activo es **muy alto** y tendría relevancia **crítica** si ocurriera la materialización de una amenaza.

- ***Criterios de valoración del Impacto Potencial total***

Para obtener el valor del Impacto Potencial total se suman los valores correspondientes al Impacto Potencial de la Integridad, Confidencialidad y Disponibilidad como se muestra en la Ecuación 2.11.

- ***Ecuación 2.11 referente al Impacto Potencial total:***

$$[I_T] = [I_i] + [I_c] + [I_d] \quad (2.11)$$

Donde,

$[I_T]$:Impacto Potencial total

En la **Tabla 2.29** se muestra la escala extendida de 15 valores, la misma que sirve de ayuda para la reducción a una escala normal de 5 valores.

Tabla 2.29. Escala de valoración del Impacto Potencial total

IMPACTO POTENCIAL TOTAL			
ESCALA EXTENDIDA	**ESCALA NORMAL**	**IMPACTO**	**DESCRIPCIÓN**
1-3	1	Muy bajo	El Impacto Potencial total del valor del activo es **muy bajo** y tendría relevancia **insignificativa** si ocurriera la materialización de una amenaza.
4-6	2	Bajo	El Impacto Potencial total del valor del activo es **bajo** y tendría relevancia **leve** si ocurriera la materialización de una amenaza.
7-9	3	Moderado	El Impacto Potencial total del valor del activo es **moderado** y tendría relevancia **significativa** si ocurriera la materialización de una amenaza.
10-12	4	Alto	El Impacto Potencial total del valor del activo es **alto** y tendría relevancia **importante** si ocurriera la materialización de una amenaza.
13-15	5	Muy alto	El Impacto Potencial total del valor del activo es **muy alto** y tendría relevancia **crítica** si ocurriera la materialización de una amenaza.

2.3.1.4. Criterios de valoración del Riesgo Potencial

2.3.1.4.1. Riesgo Potencial por dimensiones

Se denomina Riesgo Potencial a la medida del daño que se puede ocasionar a un activo de la empresa; se lo obtiene a partir de la probabilidad de ocurrencia de una amenaza sobre un activo y al Impacto Potencial de las amenazas sobre los activos [10].

El Riesgo Potencial por dimensiones es el valor resultante de la multiplicación del Impacto Potencial de cada dimensión por la probabilidad de ocurrencia, como se indica en la Ecuación 2.12.

- ***Ecuación 2.12 referente al Riesgo Potencial en Integridad:***

$$[R_i] = [I_i]x[P_O] \quad (2.12)$$

Donde,

$[R_i]$: Riesgo Potencial - Integridad

- ***Ecuación 2.13 referente al Riesgo Potencial en Confidencialidad:***

$$[R_c] = [I_c]x[P_O] \quad (2.13)$$

Donde,

$[R_c]$: Riesgo Potencial - Confidencialidad

- ***Ecuación 2.14 referente al Riesgo Potencial en Disponibilidad:***

$$[R_d] = [I_d]x[P_O] \quad (2.14)$$

Donde,

$[R_d]$: Riesgo Potencial - Disponibilidad

Una vez calculado el valor del Riesgo Potencial por cada dimensión se hace uso de una escala extendida de 25 valores, debido a que se realiza la multiplicación de dos valores con límite 5. Los resultados se muestran en una escala normal de 5 valores, como se presenta en la **Tabla 2.30**.

Tabla 2.30. Escala de valoración del Riesgo Potencial por dimensiones

RIESGO POTENCIAL POR DIMENSIONES: INTEGRIDAD, CONFIDENCIALIDAD O DISPONIBILIDAD			
ESCALA EXTENDIDA	**ESCALA NORMAL**	**IMPACTO**	**DESCRIPCIÓN**
1-5	1	Muy bajo	El Riesgo Potencial de Integridad, Confidencialidad o Disponibilidad es **muy bajo** y tendría relevancia **insignificativa** en el activo y en los objetivos de la empresa.
6-10	2	Bajo	El Riesgo Potencial de Integridad, Confidencialidad o Disponibilidad **es bajo** y tendría relevancia **leve** en el activo y en los objetivos de la empresa.
11-15	3	Moderado	El Riesgo Potencial de Integridad, Confidencialidad o Disponibilidad es **moderado** y tendría relevancia **significativa** en el activo y en los objetivos de la empresa.
16-20	4	Alto	El Riesgo Potencial de Integridad, Confidencialidad o Disponibilidad es **alto** y tendría relevancia **importante** en el activo y en los objetivos de la empresa.
21-25	5	Muy alto	El Riesgo Potencial de Integridad, Confidencialidad o Disponibilidad es **muy alto** y tendría relevancia **crítica** en el activo y en los objetivos de la empresa.

- ***Criterios de valoración del Riesgo Potencial total***

El Riesgo Potencial total es el valor resultante de la suma de los tres valores correspondientes al riesgo en cada dimensión, como se indica en la Ecuación 2.15.

- ***Ecuación 2.15 referente al Riesgo Potencial total:***

$$[R_T] = [R_i] + [R_c] + [R_d] \quad (2.15)$$

Donde,

$[R_T]$: Riesgo Potencial total

Una vez obtenido el valor del Riesgo Potencial total se hace uso de una escala extendida de 15 valores, debido a que se realiza la suma de tres valores con límite 5. Los resultados se muestran en una escala normal de 5 valores, como se presenta en la **Tabla 2.31.**

Tabla 2.31. Escala de valoración del Riesgo Potencial total

RIESGOS			
ESCALA EXTENDIDA	**ESCALA NORMAL**	**IMPACTO**	**DESCRIPCIÓN**
1-3	1	Muy bajo	El Riesgo Potencial total es **muy bajo** y tendría relevancia **insignificativa** en el activo y en los objetivos de la empresa.
4-6	2	Bajo	El Riesgo Potencial total es **bajo** y tendría relevancia **leve** en el activo y en los objetivos de la empresa.
7-9	3	Moderado	El Riesgo Potencial total es **moderado** y tendría relevancia **significativa** en el activo y en los objetivos de la empresa.
10-12	4	Alto	El Riesgo Potencial total es **alto** y tendría relevancia **importante** en el activo y en los objetivos de la empresa.
13-15	5	Muy alto	El Riesgo Potencial total es **muy alto** y tendría relevancia **crítica** en el activo y en los objetivos de la empresa.

Es importante acotar que la **Tabla 2.30** y la **Tabla 2.31** contienen las mismas escalas de valoración que se hará uso en el cálculo del Riesgo Actual y Riesgo Planificado, por lo tanto, se hará uso de esta tabla en el desarrollo de la metodología.

2.3.1.5. Criterios de valoración del Grado de Madurez o Eficacia de los Controles Existentes y Establecidos

El grado de eficacia es el valor que mide la eficacia del control existente o establecido sobre un activo frente al riesgo que protege.

Para la valoración de la eficacia se toma en cuenta el punto de vista técnico y el de operación del control [10].

En la **Tabla 2.32** se muestra a detalle el grado de madurez o eficacia de los controles, donde la columna puntos/riesgo representa al nivel de disminución del Riesgo Potencial para obtener el Riesgo Actual, así como el planificado.

Tabla 2.32. Escala de valoración de la eficacia del control existente

MADUREZ O EFICACIA DE LOS CONTROLES			
PUNTOS-RIESGO	**NIVEL**	**FACTOR**	**DESCRIPCIÓN**
0	L0	0%	La madurez del control que posee un activo es del 0%, es **inexistente**, no es técnicamente idóneo para enfrentar los riesgos que protege y no está bien desplegado o definido.
1	L1	20%	La madurez del control que posee un activo es del 20%, es **inicial** y técnicamente no está bien definido para enfrentar los riesgos que protege y sus procedimientos no son muy claros para su uso normal y en caso de incidencias.
2	L2	40%	La madurez del control que posee un activo es del 40%, es **reproducible**, pero intuitivo (deducción lógica), técnicamente tiene un nivel de definición moderado para enfrentar los riesgos que protege y sus procedimientos están claros para el uso normal y en caso de incidencias.
3	L3	60%	La madurez del control que posee un activo es del 60%, es ya un proceso **definido**, técnicamente es casi idóneo para enfrentar los riesgos que protege, está bien desplegado o definido, pero los usuarios tienen poca formación y concienciación en el tema.
4	L4	80%	La madurez del control que posee un activo es del 80%, es **gestionable y medible**, técnicamente es idóneo para enfrentar los riesgos que protege, se lo emplea casi siempre, está bien desplegado o definido, los usuarios están formados y concienciados en el tema.
5	L5	100%	La madurez del control que posee un activo es del 100%, es **optimizado**, técnicamente es idóneo para enfrentar los riesgos que protege, se lo emplea siempre, está bien desplegado o definido, los usuarios están formados y concienciados en el tema y es un control que avisa posibles fallos.

2.3.1.6. Criterios de valoración del Riesgo Actual

2.3.1.6.1. Riesgo Actual por dimensiones

Se denomina Riesgo Actual a la medida del daño que puede ocasionar a un activo de la empresa; se lo obtiene a partir del Riesgo Potencial y el valor de puntos establecidos según el nivel de madurez de los controles existentes, como se indica en las ecuaciones 2.16, 2.17 y 2.18.

- ***Ecuación 2.16 referente al Riesgo Actual - Integridad:***

$$[R_{Ai}] = [R_{Pi}] - [P_{untos}] \quad (2.16)$$

Donde,

$[R_{Ai}]$: Riesgo Actual - Integridad

- ***Ecuación 2.17 referente al Riesgo Actual - Confidencialidad:***

$$[R_{Ac}] = [R_{Pc}] - [P_{untos}] \quad (2.17)$$

Donde,

$[R_{Ac}]$: Riesgo Actual- Confidencialidad

- ***Ecuación 2.18 referente al Riesgo Actual - Disponibilidad:***

$$[R_{Ad}] = [R_{Pd}] - [P_{untos}] \quad (2.18)$$

Donde,

$[R_{Ad}]$: Riesgo Actual - Disponibilidad

Una vez calculado el valor del Riesgo Actual por cada dimensión se hace uso de la misma escala de valoración indicada en la **Tabla 2.30**, debido a que los niveles establecidos en dicha escala son los mismos para este riesgo.

- ***Criterios de valoración del Riesgo Actual total***

El Riesgo Actual total es el valor resultante de la suma de los tres valores correspondientes al riesgo en cada dimensión, como se indica en la Ecuación 2.19.

- ***Ecuación 2.19 referente la valoración del Riesgo Actual total:***

$$[R_{At}] = [R_{Ai}] + [R_{Ac}] + [R_{Ad}] \quad (2.19)$$

Donde,

$[R_{At}]$: Riesgo Actual total

Una vez obtenido el valor del Riesgo Actual total se hace uso de una escala extendida de 15 valores, como se muestra en la **Tabla 2.31** que indica los mismos niveles de valoración para este riesgo.

2.3.1.7. Criterios de valoración del Riesgo Planificado

Los criterios de valoración del Riesgo Planificado son establecidos asumiendo que la alta dirección los implementará y en el lapso de 1 año se los evaluará nuevamente.

2.3.1.8.1. Riesgo Planificado por dimensiones

Se denomina Riesgo Planificado a la medida del riesgo tratado en el lapso de un tiempo de implementación.

Para el presente análisis se considerará el lapso de 1 año, y se lo obtendrá a partir del riesgo tratado y el valor de puntos establecidos según el nivel de madurez de los controles seleccionados en el tratamiento del Riesgo Actual, como se indica en las ecuaciones 2.20, 2.21 y 2.22.

- ***Ecuación 2.20 referente al Riesgo Planificado - Integridad:***

$$[R_{Pi}] = [R_{Ai}] - [P_{untos}] \quad (2.20)$$

Donde,

$[R_{Pi}]$: Riesgo Planificado - Integridad

- ***Ecuación 2.21 referente al Riesgo Planificado - Confidencialidad:***

$$[R_{Pc}] = [R_{Ac}] - [P_{untos}] \quad (2.21)$$

Donde,

$[R_{Pc}]$: Riesgo Planificado- Confidencialidad

- ***Ecuación 2.22 referente al Riesgo Planificado - Disponibilidad:***

$$[R_{Pd}] = [R_{Ad}] - [P_{untos}] \quad (2.22)$$

Donde,

$[R_{Pd}]$: Riesgo Planificado - Disponibilidad

Una vez calculado el valor del Riesgo Planificado por cada dimensión se hace uso de la misma escala de valoración indicada en la **Tabla 2.30**, debido a que los niveles establecidos en dicha escala son los mismos para este riesgo.

- ***Criterios de valoración del Riesgo Planificado total***

El Riesgo Planificado total es el valor resultante de la suma de los tres valores correspondientes al riesgo en cada dimensión, como se indica en la ecuación 2.23

- ***Ecuación 2.23 referente la valoración del Riesgo Planificado total:***

$$[R_{Pt}] = [R_{Pi}] + [R_{Pc}] + [R_{Pd}] \quad (2.24)$$

Donde,

$[R_{Pt}]$: Riesgo Planificado total

Una vez obtenido el valor del Riesgo Planificado total se hace uso de una escala extendida de 15 valores, como se muestra en la **Tabla 2.31**, que indica los mismos niveles de valoración para este riesgo.

2.3.1.8. Criterios de aceptación y tratamiento del riesgo

En función del criterio de la alta dirección y de la matriz de Riesgo Actual, se decidirá aceptar el riesgo de nivel bajo y muy bajo; mientras que los niveles moderado, alto y muy alto se los tratará con la opción de reducción del riesgo [10].

Considerando todo lo dicho anteriormente, se establecen los criterios para la aceptación y tratamiento del Riesgo Actual, que se indican en la **Tabla 2.33**.

Tabla 2.33. Criterios de Aceptación y Tratamiento del Riesgo [10]

Aceptación y Tratamiento del Riesgo		
Rt	**Nivel**	**Acción**
1	Muy bajo	Aceptar el riesgo
2	Bajo	
3	Moderado	Reducir el riesgo
4	Alto	
5	Muy alto	

2.3.2. METODOLOGÍA DE ANÁLISIS Y GESTIÓN DE RIESGOS

Para el presente proyecto se han establecido varios pasos a seguir para el análisis y gestión de riesgos según MAGERIT [10] y la norma ISO 27001:2013 [14].

En la **Figura 2.12** se muestra un esquema de la metodología de Análisis y Gestión de riesgos, que permitirá un mejor entendimiento para el usuario.

Figura 2.12. Diagrama de flujo de la metodología de análisis y gestión de riesgos

2.3.2.1. Identificación de los activos

En la fase de identificación se realizará el levantamiento e identificación de los activos más relevantes relacionados a la seguridad de la información de la empresa Curtiembre Quisapincha.

2.3.2.1.1. Clasificación de los activos de la empresa

- ***[ESSENTIAL] Activos esenciales***

Los activos esenciales en un sistema de información son [11]:

- La información que maneja la empresa.
- Los servicios que ofrece.

En este caso se hace énfasis únicamente en la información de la empresa, debido a que es un activo crítico de la empresa.

- ***[INFO] Información***

La información es el activo esencial que la empresa maneja en el giro de negocio y es de carácter vital para el cumplimiento de los objetivos de la empresa; también posee una amplia base de datos referente a datos personales de los clientes y proveedores (ver **Tabla 2.34**).

Tabla 2.34. Activos de Información

CÓDIGO	TIPO	NOMBRE	ACTIVO	DETALLE
[INFO_VR]	[vr]	Datos Vitales	Registros confidenciales de la organización	Es la información de la empresa, referente a los reportes del sistema contable, documentación de formulaciones químicas, reportes de control de productos químicos controlados por el CONSEP.
[INFO_PER]	[per]	Datos de carácter personal	Base de datos de clientes y proveedores	Es la información confidencial referente a datos personales de clientes y proveedores
[INFO_PUB]	[pub]	Datos clasificados de carácter público	Documentación y permisos de funcionamiento	Es la información referente a permisos de funcionamiento, patentes municipales y licencia ambiental.

- ***[D]* DATOS E INFORMACIÓN COMPLEMENTARIA**

Los datos e información complementaria de la empresa son activos intangibles de la empresa que están almacenados en el servidor físico y los servidores virtuales que dispone la empresa. Los activos correspondientes a este grupo son las copias de seguridad y logs que almacenan información correspondiente a todas las áreas de la empresa (ver **Tabla 2.35**).

Tabla 2.35. Activos de Datos e Información Complementaria

CÓDIGO	TIPO	NOMBRE	ACTIVO	DETALLE
[D_BCK]	[backup]	Copias de respaldo	Copias de seguridad *OwnCloud*	La empresa realiza copias de seguridad en tiempo real, que almacena todo tipo de información generada en los servidores, en los computadores de escritorio y *laptops* que posee la empresa.
[D_LG]	[log]	Registros de actividad	Logs de SACI	La empresa cuenta con un registro de actividad del sistema contable SACI.

- ***[K] Claves criptográficas***

Las claves criptográficas son indispensables para la protección de datos de carácter público o privado. La empresa cuenta con dos activos de este grupo que permiten realizar varias actividades esenciales en la empresa y se los lista a continuación (ver **Tabla 2.36**).

Tabla 2.36. Activos de Claves Criptográficas

CÓDIGO	TIPO	NOMBRE	ACTIVO	DETALLE
[K_SIGN]	[sign]	Claves de Firma	Token digital	La empresa tiene un *token* digital, dispositivo de almacenamiento que contiene una firma digital de la empresa, y está registrada en el Banco Central.
[K_PB]	[public_ verification]	Clave pública de verificación de Firma	SSL	La empresa cuenta con un certificado SSL para brindar seguridad a los usuarios del sitio web.

- ***[S] Servicios***

Los servicios son útiles para satisfacer las necesidades de los usuarios internos y externos de la empresa. En la **Tabla 2.37** se pueden observar todos los ítems en esta categoría.

Tabla 2.37. Activos de Servicios

CÓDIGO	TIPO	NOMBRE	ACTIVO	DETALLE
[S_WWW]	[www]	World Wide Web	Sitio web	El sitio web de la empresa es www.curtiembrequisapincha.com, el cual está levantado sobre los servidores de Digital Ocean y cuenta con un certificado SSL.
[S_INT]	[int]	Interno	Servicio del sistema contable	El servicio contable que posee la empresa y de uso interno es SACI, que permite la administración contable del giro de negocio.

- ***[SW] Software- Aplicaciones informáticas***

El software disponible en la empresa automatiza algunos procesos administrativos y tecnológicos. Los activos correspondientes a este grupo se listan en la **Tabla 2.38**.

Tabla 2.38. Activos de Software – Aplicaciones Informáticas

CÓDIGO	TIPO	NOMBRE	ACTIVO	DETALLE
[SW_APP1]	[app]	Servidor de Aplicaciones	Servidor de OwnCloud	La empresa cuenta con un servidor de aplicaciones *OwnCloud* que sirve para el almacenamiento de toda la información de la empresa.
[SW_APP2]	[app]	Servidor de Aplicaciones	Servidor FTP	La empresa cuenta con un servidor FTP para realizar la transferencia de archivos referentes a anexos tributarios correspondientes al sistema de Facturación Electrónica.
[SW_APP3]	[app]	Servidor de Aplicaciones	Servidor DNS	La empresa cuenta con un servidor DNS utilizado para la traducción de dominios internos y de los servidores virtualizados.
[SW_APP4]	[app]	Servidor de Aplicaciones	Servidor Digital Ocean	La empresa aloja el sitio web en este servidor, la URL del sitio web es: www.curtiembrequisapincha.com.
[SW_WWW]	[www]	Servidor de Presentación	Servidor Web NGINX	La empresa tiene este servidor para interactuar con la página web y correo electrónico, debido a que brinda un alto nivel en velocidad de respuesta.
[SW_BD1]	[dbms]	Sistema de Gestión de Bases de Datos	Servidor de Base de Datos Oracle XE 18c	La empresa cuenta con este servidor utilizado para la administración y gestión de la base de datos del sistema contable SACI.
[SW_BD2]	[dbms]	Sistema de Gestión de Bases de Datos	Servidor de Base de Datos MySQL[21] 8.0	La empresa hace uso de este servidor para la administración y gestión del módulo de Facturación Electrónica del sistema contable SACI.
[SW_BD3]	[dbms]	Sistema de Gestión de Bases de Datos	Servidor de Base de Datos Postgresql 13	La empresa implementó este servidor para la administración y gestión de base de datos del área de recursos humanos
[SW_ALM]	[alm]	Servicio de Almacenamiento	Google Drive	La empresa cuenta con un servicio de Google en la nube, donde almacena la información en Google Drive y está relacionada a: backup de aplicaciones de todos los dispositivos móviles de la empresa, registros de las agendas de contactos; fotografías de productos, videos.
[SW_OFF]	[office]	Ofimática	Microsoft Office Professional 2019	La empresa cuenta con el paquete Microsoft Office Professional 2019, en todas las computadoras.
[SW_AV]	[av]	Antivirus	Avast Free Antivirus	La empresa utiliza el antivirus Avast Free Antivirus para todos sus equipos.
[SW_OS]	[os]	Sistema Operativo	Windows/Linux	La empresa cuenta con el sistema operativo Windows XP, 7 y 10 PRO, Linux versión de Debian 10; distribuidos en sus equipos según las necesidades de cada uno.
[SW_HP]	[hypervisor]	Gestor de Máquinas Virtuales	Proxmox	La empresa utiliza dicho entorno para la administración y gestión de sus servidores virtuales, debido a que este entorno de virtualización posee ciertas características que brindan mayor confiabilidad.

[21] MySQL: *My Structured Query Language*

- ***[Hw] Hardware- Equipos informáticos***

El hardware corresponde a todo equipo físico que brinde servicios y permita el funcionamiento de la empresa. Los activos que integran este grupo están en la **Tabla 2.39**.

Tabla 2.39. Activos de Hardware – Equipos Informáticos

CÓDIGO	TIPO	NOMBRE	ACTIVO	DETALLE
[SW_HT]	[host]	Grandes Equipos	Servidor físico HP Proliant DL 360P	Es un servidor físico sobre el cual funciona toda la estructura de red interna de la empresa, además se ejecuta la plataforma PROXMOX para la ejecución de los 7 servidores virtuales de la empresa.
[SW_PC]	[pc]	Informática personal	Computadoras de escritorio	La empresa cuenta con 8 computadoras de escritorio, distribuidas en varias áreas de la empresa.
[SW_MV1]	[movile]	Informática Móvil	Computadoras Portátiles	La empresa cuenta con 4 computadoras portátiles, distribuidas en varias áreas de la empresa.
[SW_MV2]	[movile]	Informática Móvil	Teléfonos móviles	La empresa cuenta con 12 dispositivos móviles: - 6 en el Área de Ventas. - 2 en el Área Administrativa. - 4 en el Área de Producción.
[SW_PT]	[print]	Medios de impresión	Impresoras	La empresa cuenta con - 2 impresoras multifunción que permiten la impresión y escaneo de documentos. - 4 impresoras matriciales que sirven únicamente para impresión de documentos. - 2 impresoras de etiquetas de código de barras.
[SW_SW]	[switch]	Conmutadores	*Switch* TP-LINK	La empresa cuenta con: - 2 *switches* de la marca TP-LINK que están ubicados en el *rack* del área principal de tecnología. - 6 *switches* que amplían la red interna en las diferentes áreas.
[SW_WAP]	[wap]	Punto de Acceso Inalámbrico	Punto de Acceso	La empresa cuenta con 2 puntos de acceso inalámbricos para brindar conectividad a algunas áreas de la empresa.
[SW_PB]	[pabx]	Centralita Telefónica	Central telefónica Panasonic	La empresa cuenta con una central telefónica que permite la redirección de llamadas externas hacia 4 extensiones internas, para proveer un mejor servicio a clientes y proveedores con los que se relaciona la empresa.

- ***[COM] Redes de comunicación***

Las redes de comunicación son las que brindan la conectividad entre equipos y dispositivos electrónicos. Los activos correspondientes a este grupo son los que se pueden observar en la **Tabla 2.40**.

Tabla 2.40. Activos de Redes de Comunicaciones

CÓDIGO	NOMBRE	ACTIVO	DETALLE
[COM_WF]	[wifi]	Red Inalámbrica	La empresa cuenta con dos redes Wifi: - La red principal es **outlet_curtiembre** y es libre para clientes. - La red privada para uso interno es **Red_Curtiembre.**
[COM_MB]	[mobile]	Telefonía Móvil	La empresa cuenta con 10 planes de datos para telefonía móvil.
[COM_LAN]	[LAN]	Red Local	La empresa cuenta con una red de área local, para brindar conectividad a través de cableado estructurado.
[COM_INT]	[internet]	Internet Fibra Óptica	La empresa cuenta con el servicio de Internet por fibra óptica, un servicio que es un activo esencial para la empresa, debido a que dispone de servidores virtuales en la nube.

- ***[AUX] Equipo auxiliar***

El equipo auxiliar hace referencia a todo equipo físico que sirva de soporte y no esté relacionado directamente con datos o información; sus activos se pueden apreciar con mayor detalle en la **Tabla 2.41**.

Tabla 2.41. Activos de Equipo Auxiliar

CÓDIGO	NOMBRE	ACTIVO	DETALLE
[AUX_UPS]	[ups]	Sistema de alimentación Interrumpida	La empresa cuenta con 6 UPS distribuidos varias áreas.
[AUX_AV]	[amplificador]	Amplificador de voz	La empresa hace uso de este dispositivo para amplificar la voz y transmitirla a través de los parlantes ubicados en sectores estratégicos de la empresa.
[AUX_VIDEO]	[videovigilancia]	Sistema de Video vigilancia	La empresa cuenta con un sistema de videovigilancia compuesto por 24 cámaras IP, administrados por un DVR/NVR.
[AUX_CB]	[cabling]	Cableado Estructurado	La empresa dispone de un sistema de cableado estructurado, así como de un sistema eléctrico para toda su red.

Los grupos de activos han sido seleccionados en función del inventario inicial de activos que posee la empresa y al alcance del presente proyecto de titulación.

Así también se indica que el análisis se realizará únicamente para el activo BASE DE DATOS DE CLIENTES Y PROVEEDORES correspondiente a los Activos de Información.

Los resultados detallados de la metodología de Análisis y Gestión de riesgos se indica a través de tablas en los Anexos B, C, D, E, F, G, H e I.

2.3.2.2. Valoración de activos

El objetivo de la valoración de los activos es identificar el valor de cada activo para lo cual se obtiene su costo, así como su costo por dimensión.

2.3.2.2.1. Costo del activo

El resultado del costo del activo es la suma del Costo Original y el Costo por Daño Económico.

La nomenclatura utilizada en las tablas correspondientes al costo del activo se describe a continuación:

- ✓ CO: Costo Original
- ✓ DE: Daño Económico
- ✓ CA: Costo Del Activo
- ✓ EX: Escala Extendida
- ✓ EN: Escala Normal

Para obtener el costo de cada activo se hace uso de la **Tabla 2.10.** Escala de valoración del costo original del activo y la **Tabla 2.11.** Daño económico a la empresa.

A continuación, se indica la **Tabla 2.42** de resultados del costo del activo de base de datos de clientes y proveedores.

- **[INFO] INFORMACIÓN**

Tabla 2.42. Costo del Activo: Información

COSTO DEL ACTIVO: [INFO] INFORMACIÓN						
CÓDIGO	ACTIVO	CO	DE	COSTO DEL ACTIVO		
				EX	EN	DESCRIPCIÓN
[INFO_PER]	Base de datos de clientes y proveedores	4	5	9	5	Crítico

En el ejemplo, se explica paso a paso el procedimiento a seguir para determinar el costo del activo, en este caso se tomará como muestra el activo base de datos de clientes y proveedores.

Ejemplo: Cálculo del Costo del Activo

Activo de Información: Base de datos de clientes y proveedores

Descripción:

COSTO DEL ACTIVO

- **Costo Original**

El costo original del activo es alto, es decir su implementación y levantamiento tuvo un costo inicial alto, por lo tanto, su valoración es 4, como se indica en la **Tabla 2.42.** Costo del Activo: Información.

- **Costo por daño económico a la empresa**

El costo por el daño económico por la destrucción o pérdida de un activo es muy alto, lo que podría generar graves pérdidas económicas en la empresa por lo que su valoración es 5, como se indica en la **Tabla 2.42.** Costo del Activo: Información.

- **Resultado del costo del activo**

Finalmente, una vez obtenido el costo original y el costo por daños a la empresa de dicho activo, se suman sus valores y se determina el costo del activo como se muestra a continuación (en base a la ecuación 2.1).

$$[C_A] = [C_{o,r}]+[D_E]$$

$$[C_A] = [4]+[5]$$

$$[C_{Aex}] = [9]$$

$$[C_{Aen}] = 5$$

Según la evaluación realizada se obtiene que el costo del activo es crítico en el caso de que exista pérdida o destrucción del activo y corresponde a un valor 5, que previamente se redujo de una escala extendida a una escala normal haciendo uso de la **Tabla 2.12.** Costo del Activo.

En el **ANEXO B**, se muestran las tablas de todos los activos de la empresa clasificados por grupos y su respectivo costo. (Ver desde la **Tabla B.1** hasta la **Tabla B.8**)

2.3.2.2.2. Costo por dimensiones

El costo por dimensiones se obtiene a partir de la suma de las valoraciones de cada dimensión; el valor de cada dimensión se lo obtiene en función de los 6 criterios de consecuencias seleccionados en la fase de análisis.

Para la obtención del costo por dimensiones se hacen uso de las siguientes ecuaciones ya establecidas en la fase de análisis:

- ***Ecuación 2.24 referente al valor de la Integridad:***

$$[i] = [si] + [cei] + [adm] + [lg]$$

- ***Ecuación 2.25 al valor de la Confidencialidad:***

$$[c] = [si] + [cei] + [adm] + [lg] + [rto]$$

- ***Ecuación 2.26 al valor de la Disponibilidad:***

$$[d] = [si] + [cei] + [da] + [adm] + [lg] + [rto]$$

Donde,

$[si]$: Seguridad

$[cei]$: Intereses comerciales o económicos

$[da]$: Interrupción del servicio

$[adm]$: Administración y gestión

$[lg]$: Pérdida de confianza (reputación)

$[rto]$: Tiempo de recuperación del servicio

En el **ANEXO C**, se muestra a detalle el cálculo de cada dimensión con sus respectivos criterios.

La nomenclatura utilizada en las tablas correspondientes al costo por dimensiones del activo es la siguiente:

- [i]: Valor Total de Integridad
- [c]: Valor Total de Confidencialidad
- [d]: Valor Total de Disponibilidad
- EX: Escala Extendida
- EN: Escala Normal

A continuación, se muestran los resultados de la valoración de cada dimensión y el costo por dimensiones de los activos del tipo Información, como se muestra en la **Tabla 2.43**.

- **[INFO] INFORMACIÓN**

Tabla 2.43. Costo por dimensiones del activo: Información

COSTO POR DIMENSIONES DEL ACTIVO: [INFO] INFORMACIÓN							
CÓDIGO	ACTIVO	DIMENSIONES			COSTO DIMENSIONES		
		[i]	[c]	[d]	EX	EN	NIVEL
[INFO_PER]	Base de datos de clientes y proveedores	5	5	5	15	5	CRÍTICO

Mediante un ejemplo se indica la valoración del costo del activo por dimensiones en función de sus criterios.

Ejemplo: Costo por Dimensiones del Activo

Activo de Información: Base de datos de clientes y proveedores

Descripción:

COSTO TOTAL POR DIMENSIONES

La valoraciones y cálculos obtenidos de cada criterio correspondiente a este activo se muestran a detalle en la **Tabla C.1** del **ANEXO C**.

- **Dimensión de seguridad: Integridad**

Los criterios que definen el costo en esta dimensión de seguridad son los siguientes:

Seguridad: El activo maneja información muy importante, por tanto, si existiera modificación o alteración de la información de la base de datos, probablemente podría causar un incidente muy grave en la seguridad de la información. La valoración de este criterio es muy alta y su valor es 5.

Intereses comerciales o económicos: La modificación o alteración de la información de la base de datos, podría causar pérdidas económicas fatales en la empresa y generaría gran interés comercial para la competencia. La valoración de este criterio es muy alta y su valor es 5.

Administración y gestión: El activo maneja información muy importante, por tanto, si existiera modificación o alteración de la información de la base de datos, probablemente

impediría la operación efectiva de la empresa. La valoración de este criterio es alta y su valor es de 4.

Pérdida de confianza (reputación): La alteración de la información de la base de datos, probablemente sea causa de una publicidad negativa, debido a la alteración de la información confidencial de las personas y a las relaciones con otras empresas. La valoración de este criterio es muy alta y su valor es 5.

Costo por la dimensión de Integridad

El costo de Integridad tiene un nivel de afectación muy alto con un valor en escala normal de 5 como se refiere en la **Tabla 2.20**, lo cual significa que la modificación o alteración de la información contenida en la base de datos de la empresa puede tener repercusiones fatales en la empresa.

Para obtener dicho costo se realiza la suma de las valoraciones de cada criterio como se muestra a continuación (en base a la ecuación 2.24):

$$[i] = [si] + [cei] + [adm] + [lg]$$

$$[iex] = [5] + [5] + [4] + [5]$$

$$[iex] = [19]$$

$$[in] = [5]$$

Donde,

i_{ex}: Costo de Integridad en escala extendida.

i_n: Costo de Integridad en escala normal o reducida.

Por lo tanto, para llegar a un valor en escala normal se hace uso de la **Tabla 2.20.** Escala Valoración de la INTEGRIDAD.

- **Dimensión de seguridad: Confidencialidad**

Los criterios que definen el costo en esta dimensión de seguridad son los siguientes:

Seguridad: El activo maneja información muy importante, por tanto, si las bases de datos fuesen reveladas o divulgadas, podría causar un incidente muy grave en la seguridad de la información. La valoración de este criterio es muy alta y su valor es 5.

Intereses comerciales o económicos: La información que contiene la base de datos es muy importante, por tanto, si existiera revelación o divulgación de la información de dicha base

de datos, podría causar pérdidas económicas fatales en la empresa y generaría gran interés comercial para la competencia. La valoración de este criterio es muy alta y su valor es 5.

Administración y gestión: Si la información contenida en la base de datos fuese revelada o divulgada, impediría la operación efectiva de la empresa. La valoración de este criterio es muy alta y su valor es de 5.

Pérdida de confianza (reputación): La divulgación o revelación de la base de datos de clientes y proveedores podría ocasionar publicidad negativa debido a la filtración de datos confidenciales de las personas y esto afectaría a las relaciones con otras empresas. La valoración de este criterio es muy alta y su valor es 5.

Tiempo de recuperación del servicio: La divulgación o revelación de la información contenida en la base de datos de clientes y proveedores podría alterar su funcionamiento y ocasionar un RTO menor a 2 horas, lo que significa que los servicios y sistemas administrativos no podrían continuar su funcionamiento normal y generarían pérdidas económicas para la empresa. La valoración de este criterio es muy alta y su valor es 5.

Costo por la dimensión de Confidencialidad

El costo de Confidencialidad tiene un nivel de afectación muy alto con un valor en escala normal de 5 como se refiere en la **Tabla 2.21**, lo cual significa que la divulgación de la información del activo es de uso secreto y podría tener un nivel de afectación fatal para la economía de la empresa.

Para obtener dicho costo se realiza la suma de las valoraciones de cada criterio como se muestra a continuación (en base a la ecuación 2.25):

$$[c] = [si] + [cei] + [adm] + [lg] + [rto]$$

$$[cex] = [5] + [5] + [5] + [5] + [5]$$

$$[cex] = [25]$$

$$[cn] = [5]$$

Donde,

c_{ex}: significa el costo de Confidencialidad en escala extendida.

c_n: significa el costo de Confidencialidad en escala normal o reducida.

Por lo tanto, para llegar a un valor en escala normal se hace uso de la **Tabla 2.21.** Escala de valoración de la CONFIDENCIALIDAD.

- **Dimensión de seguridad: Disponibilidad**

Los criterios que definen el costo en esta dimensión de seguridad son los siguientes:

Seguridad: El activo maneja información muy importante, por tanto, si las bases de datos no estuviesen disponibles, podría ocasionar un incidente muy grave en la seguridad de la información. La valoración de este criterio es muy alta y su valor es 5.

Intereses comerciales o económicos: La información que contiene la base de datos es muy importante, por tanto, si dicha base de datos no está disponible las pérdidas económicas de la empresa serian fatales y generaría gran interés comercial para la competencia. La valoración de este criterio es muy alta y su valor es 5.

Interrupción del servicio: Si el activo que contiene información de clientes y proveedores no está disponible, podría interrumpir todas las actividades de los procesos administrativos de la empresa. La valoración de este criterio es muy alta y su valor es 5.

Administración y gestión: La base de datos de clientes y proveedores es uno de los activos esenciales de la empresa, por lo tanto, la pérdida o destrucción de esta, probablemente impediría la operación efectiva de varios procesos de la empresa. La valoración de este criterio es alta y su valor es de 4.

Pérdida de confianza (reputación): La indisponibilidad de la base de datos de clientes y proveedores podría ocasionar publicidad negativa debido a que se puede generar la caída del sistema y esto afectaría a la relación con los clientes. La valoración de este criterio es muy alta y su valor es 5.

Tiempo de recuperación del servicio: La indisponibilidad del activo que contiene información de clientes y proveedores podría ocasionar un RTO menor a 2 horas, lo que significa que los servicios y sistemas administrativos no podrían continuar su funcionamiento normal y generarían pérdidas económicas para la empresa. La valoración de este criterio es muy alta y su valor es 5.

Costo por la dimensión de Disponibilidad

El costo de disponibilidad tiene un nivel de afectación muy alto con un valor en escala normal de 5 como se refiere en la **Tabla 2.22**, lo cual significa que la destrucción o indisponibilidad del activo tendría un impacto total sobre la empresa.

Para obtener dicho costo se realiza la suma de las valoraciones de cada criterio como se muestra a continuación (en base a la ecuación 2.26):

$$[d] = [si] + [cei] + [da] + [adm] + [lg] + [rto]$$

$$[dex] = [5] + [5] + [5] + [4] + [5] + [5]$$

$$[dex] = [29]$$

$$[dn] = [5]$$

Donde,

$[dex]$: significa el costo de disponibilidad en escala extendida.

$[dn]$: significa el costo de disponibilidad en escala normal o reducida.

Por lo tanto, para llegar a un valor en escala normal se hace uso de la **Tabla 2.22.** Escala de valoración de la DISPONIBILIDAD.

- **Resultado del costo total por dimensiones**

El costo total por dimensiones corresponde a la suma de los valores obtenidos en cada dimensión, como se indica a continuación (en base a la ecuación 2.5):

$$[C_{Td}] = [Vt_i] + [Vt_c] + [Vt_d]$$

$$[C_{Td}] = [5] + [5] + [5]$$

$$[C_{Td}] = [5]$$

El costo total por dimensiones de la base de datos de clientes y proveedores es crítico, en el caso de que exista pérdida de Integridad, Confidencialidad y Disponibilidad de la información; su valoración es igual a 5, valor obtenido de la suma de sus 3 dimensiones y reducido a una escala normal como se indica en la **Tabla 2.23.** Costo total por dimensiones.

En el **ANEXO C** se listan todos los activos de la empresa clasificados por grupos y su respectivo costo total por dimensiones (Ver desde la **Tabla C.1** hasta la **Tabla C.8**.).

2.3.2.2.3. Valor del activo

Una vez obtenido el costo del activo y el costo por dimensiones, se determinará el valor del activo, mediante la suma del costo del activo y el costo por dimensiones de seguridad, como se indica a continuación (en base a la ecuación 2.6):

$$[V_A] = [C_{Ta}] + [C_{Td}]$$

$$[V_A] = [5] + [5]$$

$$[V_{Aex}] = [10]$$

$$[V_{Aen}] = [5]$$

El valor del activo de la base de datos de clientes y proveedores es muy alto, por lo tanto, tiene relevancia crítica en la empresa; es decir, su pérdida o alteración podría causar pérdidas económicas o de reputación a la empresa. Como se indica en la **Tabla 2.24.** Valor del activo, el valor corresponde a 5 en su escala reducida.

- **[INFO] INFORMACIÓN**

Tabla 2.44. Valor del Activo: Información

VALOR DEL ACTIVO: [INFO] INFORMACIÓN						
CÓDIGO	**ACTIVO**	**COSTO DEL ACTIVO**	**COSTO POR DIMENSIONES**	**VALOR ACTIVO**		
				EX	**EN**	**DESCRIPCIÓN**
[INFO_PER]	Base de datos de clientes y proveedores	5	5	10	5	MUY ALTO

En el **ANEXO D** se muestra a detalle los resultados obtenidos del valor de cada activo. (Ver desde la **Tabla D.1** hasta la **Tabla D.8**).

2.3.1.3. Identificación y valoración de Amenazas

Para la identificación de amenazas se hace uso del catálogo de amenazas del Libro II de MAGERIT v.3 [11]. En base a las características de cada grupo de activos, se seleccionan las amenazas que puedan afectar directamente a los activos de la empresa.

En la **Tabla 2.45**., se muestran los resultados obtenidos de la identificación y valoración de las amenazas del activo base de datos de clientes y proveedores, del cual se realizará el análisis de los resultados en esta sección.

- **INFORMACIÓN: [INFO_PER]**

Tabla 2.45. Matriz de identificación y valoración de amenazas [INFO_PER]

[INFO] INFORMACIÓN									
[INFO_PER]	**Base de datos de clientes y proveedores**								
TIPO DE AMENAZAS	**AMENAZAS**	**Dv: DEGRADACIÓN DE VALOR POR DIMENSIONES**						**PROBABILIDAD DE OCURRENCIA**	
		Dv-i	**Dv-c**	**Dv-d**	**Dt-ex**	**DT**	**NIVEL**	**Po**	**NIVEL**
5.3. [E] Errores y fallos no intencionados	5.3.1. [E.1] Errores de los usuarios	4	4	4	12	4	ALTO	5	MUY FRECUENTE
	5.3.2. [E.2] Errores del administrador	5	5	5	15	5	MUY ALTO	5	MUY FRECUENTE
	5.3.10. [E.15] Alteración accidental de la información	5	4	4	13	5	MUY ALTO	3	NORMAL
	5.3.11. [E.18] Destrucción de información	3	5	5	13	5	MUY ALTO	3	NORMAL
	5.3.12. [E.19] Fugas de información	5	5	4	14	5	MUY ALTO	4	FRECUENTE
5.4. [A] Ataques intencionados	5.4.3. [A.5] Suplantación de la identidad del usuario	5	5	1	11	4	ALTO	3	NORMAL
	5.4.4. [A.6] Abuso de privilegios de acceso	3	3	5	11	4	ALTO	2	POCO FRECUENTE
	5.4.9. [A.11] Acceso no autorizado	4	5	3	12	4	ALTO	3	NORMAL
	5.4.13. [A.15] Modificación deliberada de la información	5	4	2	11	4	ALTO	2	POCO FRECUENTE
	5.4.15. [A.19] Divulgación de información	4	5	1	10	4	ALTO	4	FRECUENTE

Ejemplo: Identificación de amenazas

Activo de Información: Base de datos de clientes y proveedores

Descripción: Para el activo analizado la base de datos de clientes y proveedores corresponde al grupo de activo de información, por lo tanto, se han identificado que este activo podría ser afectado por 2 tipos de amenazas:

- **Errores y fallos no intencionados**

Este tipo de amenazas afectan directamente al activo debido a que la información que se maneja en dicha base de datos está administrada por varios usuarios y el administrador, quienes pueden ocasionar daños o alteraciones accidentales. A continuación, se listan las amenazas seleccionadas para el análisis de riesgos:

- Errores de los usuarios
- Errores del administrador
- Alteración accidental de la información
- Destrucción de información
- Fugas de información

- **Ataques intencionados**

Los ataques intencionados representan a un tipo de amenazas que podrían afectar a todos los activos, en este caso se tiene varias amenazas que afectan a la base de datos de clientes y proveedores. Dichas amenazas pueden ser las siguientes:

- Suplantación de la identidad del usuario
- Abuso de privilegios de acceso
- Acceso no autorizado
- Modificación deliberada de la información
- Divulgación de información

Las amenazas listadas son las que podrían afectar directamente al activo, sin embargo, pueden existir más amenazas que lo acechen.

Ejemplo: Valoración de amenazas

Activo de Información: Base de datos de clientes y proveedores

Tipo de Amenaza: Errores y fallos no intencionados

Amenaza: Errores de los usuarios

Descripción:

- **Degradación de Valor por Dimensiones**

Como objeto de análisis se ha seleccionado el tipo de amenaza correspondiente a errores y fallos no intencionados, del cual se selecciona la amenaza errores de los usuarios. Se ha seleccionada esta amenaza debido a que la empresa no cuenta con una adecuada gestión de accesos a las bases de datos, no existen usuarios específicos que tengan acceso al sistema.

En la **Tabla 2.45.** Matriz de identificación y valoración de amenazas [INFO_PER] se indican los resultados del análisis de las amenazas en función de su degradación según cada dimensión.

La degradación de valor en función de la *Integridad* ha sido valorada con un nivel alto y un valor 4, debido a que el error de un usuario puede causar la alteración de los datos del activo, si este no tiene el conocimiento que requiere para el tratamiento del activo en cuestión.

La degradación de valor en función de la *Confidencialidad* ha sido valorada con un nivel alto y un valor 4, debido a que el error de un usuario puede vulnerar la información de la base de datos y a su vez ser divulgada por personal no autorizado.

La degradación de valor en función de la *Disponibilidad* ha sido valorada con un nivel alto y un valor 4, debido a que el error de un usuario puede causar indisponibilidad de la información contenida en la base de datos de los clientes y proveedores.

La degradación de valor total corresponde a la suma de las degradaciones de cada dimensión como se muestra a continuación (en base a la ecuación 2.7).

$$[D_T] = [D_{v-i}] + [D_{v-c}] + [D_{v-d}]$$

$$[D_T] = [4] + [4] + [4]$$

$$[D_{Tex}] = [12]$$

$$[D_{Ten}] = [4]$$

Donde,

$[D_{Tex}]$: Degradación de valor total en escala extendida.

$[D_{Ten}]$: Degradación de valor total en escala normal.

El resultado de la degradación de valor total en escala extendida es de 12, lo cual en una escala normal tiene un valor igual a 4 que corresponde al nivel alto como se indica en la **Tabla 2.26.** Degradación total. Es decir, que, si existiera un daño en el activo a causa de un incidente, es muy alta la posibilidad de que le ocasione una degradación total.

- **Probabilidad de Ocurrencia**

La probabilidad de ocurrencia de que el error de un usuario se materialice es muy frecuente, es decir, que podría suceder a diario, por lo que se le ha asignado un valor de 5 según la **Tabla 2.27.** Probabilidad de ocurrencia, debido a que la empresa no cuenta con un proceso o una gestión de accesos adecuada.

En el **ANEXO E**, se listan todos los activos con las amenazas identificadas y sus respectivas valoraciones. (Ver de la **Tabla E.1** hasta la **Tabla E.36**)

2.3.1.4. Valoración del Impacto Potencial

El Impacto Potencial es el valor obtenido a través del valor del activo y de la degradación de valor en cada dimensión, sin tomar en cuenta los controles existentes que la empresa posea.

En la **Tabla 2.46**., se muestra los resultados obtenidos del Impacto Potencial, tanto en sus dimensiones como el Impacto Total.

- **INFORMACIÓN: [INFO_PER]**

Tabla 2.46. Valoración del Impacto Potencial [INFO_PER]

[INFO] INFORMACIÓN					
[INFO_PER]	**Base de datos de clientes y proveedores**				
AMENAZAS	**IMPACTO POTENCIAL**				
	I: IMPACTO POTENCIAL POR DIMENSIONES			**IMPACTO TOTAL**	
	Ii	**Ic**	**Id**	**I-TOTAL**	**NIVEL**
5.3.1. [E.1] Errores de los usuarios	4	4	4	4	ALTO
5.3.2. [E.2] Errores del administrador	5	5	5	5	MUY ALTO
5.3.10. [E.15] Alteración accidental de la información	5	4	4	5	MUY ALTO
5.3.11. [E.18] Destrucción de información	3	5	5	5	MUY ALTO
5.3.12. [E.19] Fugas de información	5	5	4	5	MUY ALTO
5.4.3. [A.5] Suplantación de la identidad del usuario	5	5	1	4	ALTO
5.4.4. [A.6] Abuso de privilegios de acceso	3	3	5	4	ALTO
5.4.9. [A.11] Acceso no autorizado	4	5	3	4	ALTO
5.4.13. [A.15] Modificación deliberada de la información	5	4	2	4	ALTO
5.4.15. [A.19] Divulgación de información	4	5	1	4	ALTO

En el siguiente ejemplo se realiza un análisis a detalle cada valor obtenido referente al activo de base de datos de los clientes y proveedores, con una amenaza y su respectiva degradación y probabilidad de ocurrencia.

Ejemplo: Valoración del Impacto Potencial

Activo de Información: Base de datos de clientes y proveedores

Tipo de Amenaza: Errores y fallos no intencionados

Amenaza: Errores de los usuarios

Descripción:

- **Impacto Potencial por Dimensiones**

El Impacto Potencial por dimensiones es igual al nivel de degradación en cada dimensión por el valor del activo, sin tomar en cuenta los controles existentes.

El Impacto Potencial en función de la Integridad, Confidencialidad y Disponibilidad ha sido obtenido a través de la multiplicación del valor del activo por la degradación de valor de Integridad, Confidencialidad y Disponibilidad; en este caso dichos valores corresponden a 5 y 4, 4, 4, respectivamente.

El Impacto Potencial en todas sus dimensiones es igual a 20, lo que en escala reducida da un valor de 4; según la **Tabla 2.28.** Escala de valoración del Impacto Potencial por dimensiones, corresponde el impacto a un valor del activo alto y tendría relevancia importante si ocurriera la materialización de una amenaza.

El Impacto Potencial total corresponde a la suma de los impactos en cada dimensión como se muestra a continuación (en base a la ecuación 2.11):

$$[I_T] = [I_i] + [I_c] + [I_d]$$

$$[I_T] = [4] + [4] + [4]$$

$$[I_{Tex}] = [12]$$

$$[I_{Ten}] = [4]$$

Donde,

$[I_{Tex}]$: significa el Impacto Potencial total en escala extendida.

$[I_{Ten}]$: significa el Impacto Potencial total en escala normal.

El resultado del impacto potencial total en escala extendida es 12, lo cual se reduce a una escala normal y se tiene un valor igual a 4 que corresponde al nivel alto como se indica en la **Tabla 2.29.** Escala de valoración del Impacto Potencial total.

En el Anexo F se listan todos los activos con sus respectivos resultados de la valoración del Impacto Potencial por dimensiones e impacto potencial total. (Ver **Tabla F.1** hasta la **Tabla F.36**)

2.3.1.5. Valoración del Riesgo Potencial

El Riesgo Potencial es el valor obtenido a través de la probabilidad de ocurrencia del activo y el Impacto Potencial en cada dimensión, sin tomar en cuenta los controles existentes que la empresa posea.

En la **Tabla 2.47** se observan los resultados obtenidos del Riesgo Potencial por dimensiones y total.

- **INFORMACIÓN: [INFO_PER]**

Tabla 2.47. Valoración del Riesgo Potencial [INFO_PER]

[INFO] INFORMACIÓN					
[INFO_PER]	**Base de datos de clientes y proveedores**				
AMENAZAS	**RIESGO POTENCIAL**				
	RIESGO POTENCIAL POR DIMENSIONES			**RIESGO POTENCIAL TOTAL**	
	Ri	**Rc**	**Rd**	**Rt**	**NIVEL**
5.3.1. [E.1] Errores de los usuarios	4	4	4	4	ALTO
5.3.2. [E.2] Errores del administrador	5	5	5	5	MUY ALTO
5.3.10. [E.15] Alteración accidental de la información	3	3	3	3	MODERADO
5.3.11. [E.18] Destrucción de información	2	3	3	3	MODERADO
5.3.12. [E.19] Fugas de información	4	4	4	4	ALTO
5.4.3. [A.5] Suplantación de la identidad del usuario	3	3	1	3	MODERADO
5.4.4. [A.6] Abuso de privilegios de acceso	2	2	2	2	BAJO
5.4.9. [A.11] Acceso no autorizado	3	3	2	3	MODERADO
5.4.13. [A.15] Modificación deliberada de la información	2	2	1	2	BAJO
5.4.15. [A.19] Divulgación de información	4	4	1	3	MODERADO

En la siguiente sección se muestran un análisis de los resultados de la valoración del Riesgo Potencial de los activos considerados para objeto de análisis.

Ejemplo: Valoración del Riesgo Potencial

Activo de Información: Base de datos de clientes y proveedores

Tipo de Amenaza: Errores y fallos no intencionados

Amenaza: Errores de los usuarios

Descripción:

- **Riesgo Potencial por Dimensiones**

El Riesgo Potencial en todas sus dimensiones es igual a 25, que en su escala reducida da un valor de 5; según la **Tabla 2.30.** Escala de valoración del Riesgo Potencial por dimensiones corresponde, el impacto en el valor del activo, a muy alto y tendría relevancia crítica si ocurriera la materialización de una amenaza.

El Riesgo Potencial total corresponde a la suma de los impactos en cada dimensión como se muestra a continuación (en base a la ecuación 2.15):

$$[R_T] = [R_i] + [R_c] + [R_d]$$

$$[R_T] = [5] + [5] + [5]$$

$$[R_{Tex}] = [15]$$

$$[R_{Ten}] = [5]$$

Donde,

$[R_{Tex}]$: significa el Riesgo Potencial total en escala extendida.

$[R_{Ten}]$: significa el Riesgo Potencial total en escala normal.

El resultado del Riesgo Potencial total en escala extendida es de 15, lo cual se reduce a una escala normal y se tiene un valor igual a 5 que corresponde a un nivel muy alto, como se indica en la **Tabla 2.31**.

En el **ANEXO G**, se listan todos los activos con sus respectivos resultados de la valoración del Riesgo Potencial por dimensiones y Riesgo Potencial total. (Ver desde la **Tabla G.1** hasta la **Tabla G.36**)

2.3.1.6. Elaboración del Documento de Aplicabilidad (SOA)

En el presente proyecto, en el documento de aplicabilidad se establecen los controles necesarios para la gestión de riesgos; será elaborado en función del Anexo A de la ISO27001:2013, el alcance y las limitaciones del Sistema de Gestión de Seguridad de la Información.

De la **Tabla 2.48** a la **Tabla 2.61** se muestra a detalle en cada una de ellas los 14 dominios con sus respectivos objetivos de control y controles respectivamente. Mediante la evaluación de aplicabilidad se determina que, de los 114 controles establecidos por la ISO 27001:2013, 64 de ellos si aplican para la gestión de riesgos y los 50 restantes no aplican debido a la definición del alcance del SGSI.

Tabla 2.48. Documento de aplicabilidad relacionado a políticas de seguridad de la Información

A.5 POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN			
CONTROL		**APLICA**	**OBSERVACIONES**
A.5.1 Dirección de gestión de seguridad de la información			
A.5.1.1	Políticas para la seguridad de la información.	SI	Aplica porque este control está incluido en el alcance del SGSI.
A.5.1.2	Revisión de las políticas para la seguridad de la información.	SI	Aplica porque este control está incluido en el alcance del SGSI.

Tabla 2.49. Documento de aplicabilidad relacionado a la organización de la seguridad de la información

A.6 ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN			
CONTROL		**APLICA**	**OBSERVACIONES**
A.6.1 Organización interna			
A.6.1.1	Roles y responsabilidades de seguridad de la información.	SI	Aplica porque este control está incluido en el alcance del SGSI.
A.6.1.2	Separación de funciones.	SI	Aplica porque este control está incluido en el alcance del SGSI.
A.6.1.3	Contacto con las autoridades.	SI	Aplica porque este control está incluido en el alcance del SGSI.
A.6.1.4	Contacto con grupos de interés especial.	SI	Aplica porque este control está incluido en el alcance del SGSI.
A.6.1.5	Gestión de proyectos de seguridad de la información.	SI	Aplica porque este control está incluido en el alcance del SGSI.
A.6.2 Dispositivos móviles y teletrabajo			
A.6.2.1	Política de dispositivo móvil.	SI	Aplica porque este control está incluido en el alcance del SGSI.
A.6.2.2	Teletrabajo.	NO	No aplica porque no se realiza la actividad dentro de la empresa.

Tabla 2.50. Documento de aplicabilidad relacionado a seguridad en Recursos Humanos

A.7 SEGURIDAD EN RECURSOS HUMANOS			
CONTROL		**APLICA**	**OBSERVACIONES**
A.7.1 Antes del empleo			
A.7.1.1	Investigación de antecedentes.	NO No aplica, porque está fuera del alcance del SGSI.	
A.7.1.2	Términos y condiciones del empleo.	NO	No aplica, porque está fuera del alcance del SGSI.
A.7.2 Durante el empleo			
A.7.2.1	Responsabilidades de la dirección.	NO	No aplica, porque está fuera del alcance del SGSI.
A.7.2.2	Concienciación, educación y capacitación en seguridad de la información.	NO	No aplica, porque está fuera del alcance del SGSI.
A.7.2.3	Proceso disciplinario.	NO	No aplica, porque está fuera del alcance del SGSI.
A.7.3 Finalización o cambio de empleo			
A.7.3.1	Responsabilidades ante la finalización o cambio de empleo.	NO	No aplica, porque está fuera del alcance del SGSI.

Tabla 2.51. Documento de aplicabilidad relacionado a la Gestión de Activos

A.8 GESTIÓN DE ACTIVOS			
CONTROL		**APLICA**	**OBSERVACIONES**
A.8.1 Responsabilidad de los activos			
A.8.1.1	Inventario de activos.	SI	Aplica porque este control está incluido en el alcance del SGSI.
A.8.1.2	Propiedad de los activos.	SI	Aplica porque este control está incluido en el alcance del SGSI.
A.8.1.3	Uso aceptable de los activos.	SI	Aplica porque este control está incluido en el alcance del SGSI.
A.8.1.4	Devolución de activos.	SI	Aplica porque este control está incluido en el alcance del SGSI.
A.8.2 Clasificación de la información			
A.8.2.1	Clasificación de la información.	SI	Aplica porque este control está incluido en el alcance del SGSI.
A.8.2.2	Etiquetado de la información.	SI	Aplica porque este control está incluido en el alcance del SGSI.
A.8.2.3	Manejo de los activos.	SI	Aplica porque este control está incluido en el alcance del SGSI.
A.8.3 Manejo de los medios			
A.8.3.1	Gestión de medios extraíbles.	SI	Aplica porque este control está incluido en el alcance del SGSI.
A.8.3.2	Eliminación de los medios.	SI	Aplica porque este control está incluido en el alcance del SGSI.
A.8.3.3	Transferencia de medios físicos.	SI	Aplica porque este control está incluido en el alcance del SGSI.

Tabla 2.52. Documento de aplicabilidad relacionado al Control de Acceso

A.9 CONTROL DE ACCESO			
CONTROL		**APLICA**	**OBSERVACIONES**
A.9.1 Requisitos de negocio para el control de acceso			
A.9.1.1	Política de control de accesos.	SI	Aplica porque este control está incluido en el alcance del SGSI.
A.9.1.2	Control de acceso a las redes y servicios asociados.	SI	Aplica porque este control está incluido en el alcance del SGSI.
A.9.2 Gestión de acceso de los usuarios			
A.9.2.1	Registro y retiro de usuario.	SI	Aplica porque este control está incluido en el alcance del SGSI.
A.9.2.2	Provisión de accesos a usuarios.	SI	Aplica porque este control está incluido en el alcance del SGSI.
A.9.2.3	Gestión de privilegios de derechos de acceso.	SI	Aplica porque este control está incluido en el alcance del SGSI.
A.9.2.4	Gestión de la información secreta de autenticación de los usuarios.	SI	Aplica porque este control está incluido en el alcance del SGSI.
A.9.2.5	Revisión de los derechos de acceso de usuario.	SI	Aplica porque este control está incluido en el alcance del SGSI.
A.9.2.6	Retiro y ajuste de los derechos de acceso.	SI	Aplica porque este control está incluido en el alcance del SGSI.
A.9.3 Responsabilidades del usuario			
A.9.3.1	Uso de la información secreta de autenticación.	SI	Aplica porque este control está incluido en el alcance del SGSI.
A.9.4 Control de acceso a sistemas y aplicaciones			
A.9.4.1	Restricción del acceso a la información.	SI	Aplica porque este control está incluido en el alcance del SGSI.
A.9.4.2	Procedimientos seguros de inicio de sesión.	SI	Aplica porque este control está incluido en el alcance del SGSI.
A.9.4.3	Sistema de gestión de contraseñas.	SI	Aplica porque este control está incluido en el alcance del SGSI.
A.9.4.4	Uso de programas utilitarios privilegiados.	NO	No, porque la empresa no cuenta con este tipo de sistemas.
A.9.4.5	Control de acceso al código fuente del programa.	NO	No, porque no cuenta con código fuente de programas.

Tabla 2.53. Documento de aplicabilidad relacionado a Criptografía

A.10 CRIPTOGRAFÍA			
CONTROL		**APLICA**	**OBSERVACIONES**
A.10.1 Controles criptográficos			
A.10.1.1	Política de uso de los controles criptográficos.	SI	Aplica porque este control está incluido en el alcance del proyecto.
A.10.1.2	Gestión de Llaves.	SI	Aplica porque este control está incluido en el alcance del proyecto.

Tabla 2.54. Documento de aplicabilidad relacionado a la seguridad física y del entorno

A.11 SEGURIDAD FÍSICA Y DEL ENTORNO			
CONTROL		**APLICA**	**OBSERVACIONES**
A.11.1 Áreas seguras			
A.11.1.1	Perímetro de seguridad física.	NO	No aplica, porque está fuera del alcance del SGSI.
A.11.1.2	Controles físicos de entrada.	NO	No aplica, porque está fuera del alcance del SGSI.
A.11.1.3	Seguridad de oficinas, despachos e instalaciones.	NO	No aplica, porque está fuera del alcance del SGSI.
A.11.1.4	Protección contra las amenazas externas y ambientales.	NO	No aplica, porque está fuera del alcance del SGSI.
A.11.1.5	El trabajo en áreas seguras.	NO	No aplica, porque está fuera del alcance del SGSI.
A.11.1.6	Áreas de carga y entrega.	NO	No aplica, porque está fuera del alcance del SGSI.
A.11.2 Equipos			
A.11.2.1	Ubicación y protección de equipos.	NO	No aplica, porque está fuera del alcance del SGSI.
A.11.2.2	Instalaciones de suministro.	NO	No aplica, porque está fuera del alcance del SGSI.
A.11.2.3	Seguridad del cableado.	NO	No aplica, porque esta fuera del alcance del SGSI.
A.11.2.4	Mantenimiento de los equipos.	NO	No aplica, porque está fuera del alcance del SGSI.
A.11.2.5	Eliminación de activos	NO	No aplica, porque está fuera del alcance del SGSI.
A.11.2.6	Seguridad de los equipos y activos fuera de las instalaciones.	NO	No aplica, porque está fuera del alcance del SGSI.
A.11.2.7	Reutilización o eliminación segura de equipos.	NO	No aplica, porque está fuera del alcance del SGSI.
A.11.2.8	Equipo de usuario desatendido.	NO	No aplica, porque está fuera del alcance del SGSI.
A.11.2.9	Política de puesto de trabajo despejado y pantalla limpia.	NO	No aplica, porque está fuera del alcance del SGSI.

Tabla 2.55. Documento de aplicabilidad relacionado a la seguridad de las operaciones

A.12 SEGURIDAD DE LAS OPERACIONES			
CONTROL		**APLICA**	**OBSERVACIONES**
A.12.1 Procedimientos y responsabilidades operacionales			
A.12.1.1	Documentación de procedimientos de operación.	SI	Aplica porque este control está incluido en el alcance del SGSI.
A.12.1.2	Gestión de cambios.	SI	Aplica porque este control está incluido en el alcance del SGSI.
A.12.1.3	Gestión de capacidades.	SI	Aplica porque este control está incluido en el alcance del SGSI.
A.12.1.4	Separación de ambientes de desarrollo, pruebas y producción.	SI	Aplica porque este control está incluido en el alcance del SGSI.
A.12.2 Protección contra un malware			
A.12.2.1	Controles contra un *malware.*	SI	Aplica porque este control está incluido en el alcance del SGSI.
A.12.3 Copias de seguridad			
A.12.3.1	Copias de seguridad de la información.	SI	Aplica porque este control está incluido en el alcance del SGSI.
A.12.4 Registro y monitoreo			
A.12.4.1	Registro de eventos.	SI	Aplica porque este control está incluido en el alcance del SGSI.
A.12.4.2	Protección de la información de registro.	SI	Aplica porque este control está incluido en el alcance del SGSI.
A.12.4.3	Registros de administración y operación.	SI	Aplica porque este control está incluido en el alcance del SGSI.
A.12.4.4	Sincronización del reloj.	SI	Aplica porque este control está incluido en el alcance del SGSI.
A.12.5 Control del software operacional			
A.12.5.1	Instalación del software en los sistemas operativos.	SI	Aplica porque este control está incluido en el alcance del SGSI.
A.12.6 Gestión de la vulnerabilidad técnica			
A.12.6.1	Gestión de vulnerabilidades técnicas.	SI	Aplica porque este control está incluido en el alcance del SGSI.
A.12.6.2	Restricciones en la instalación del software.	SI	Aplica porque este control está incluido en el alcance del SGSI.
A.12.7 Consideraciones sobre la auditoría de sistemas de información			
A.12.7.1	Controles de auditoría de los sistemas de información.	SI	Aplica porque este control está incluido en el alcance del SGSI.

Tabla 2.56. Documento de aplicabilidad relacionado a la seguridad en las comunicaciones

A.13 SEGURIDAD EN LAS COMUNICACIONES			
CONTROL		**APLICA**	**OBSERVACIONES**
A.13.1 Gestión de la seguridad de redes			
A.13.1.1	Controles de red.	SI	Aplica porque este control está incluido en el alcance del SGSI.
A.13.1.2	Seguridad de los servicios de red.	SI	Aplica porque este control está incluido en el alcance del SGSI.
A.13.1.3	Separación en las redes.	SI	Aplica porque este control está incluido en el alcance del SGSI.
A.13.2 Transferencia de información			
A.13.2.1	Políticas y procedimientos de transferencia de información.	SI	Aplica porque este control está incluido en el alcance del SGSI.
A.13.2.2	Acuerdos de transferencia de información.	SI	Aplica porque este control está incluido en el alcance del SGSI.
A.13.2.3	Mensajería electrónica.	SI	Aplica porque este control está incluido en el alcance del SGSI.
A.13.2.4	Acuerdos de confidencialidad o no revelación.	SI	Aplica porque este control está incluido en el alcance del SGSI.

Tabla 2.57. Documento de aplicabilidad relacionado a la adquisición, desarrollo y mantenimiento del sistema

A.14 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DEL SISTEMA			
CONTROL		**APLICA**	**OBSERVACIONES**
A.14.1 Requisitos de seguridad de los sistemas de información			
A.14.1.1	Análisis de requisitos y especificaciones de seguridad de la información.	NO	No aplica, porque en el giro de negocio de la empresa no se realiza desarrollo de sistemas.
A.14.1.2	Asegurar los servicios de aplicaciones en redes públicas.	NO	No aplica, porque en el giro de negocio de la empresa no se realiza desarrollo de sistemas.
A.14.1.3	Protección de las transacciones de servicios de aplicaciones.	NO	No aplica, porque en el giro de negocio de la empresa no se realiza desarrollo de sistemas.
A.14.2 Seguridad en el desarrollo y en los procesos de soporte			
A.14.2.1	Política de desarrollo seguro.	NO	No aplica, porque en el giro de negocio de la empresa no se realiza desarrollo de sistemas.
A.14.2.2	Procedimientos de control de cambios en sistemas.	NO	No aplica, porque en el giro de negocio de la empresa no se realiza desarrollo de sistemas.
A.14.2.3	Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo.	NO	No aplica, porque en el giro de negocio de la empresa no se realiza desarrollo de sistemas.
A.14.2.4	Restricciones a los cambios en los paquetes de software.	NO	No aplica, porque en el giro de negocio de la empresa no se realiza desarrollo de sistemas.
A.14.2.5	Principios de ingeniería de sistemas seguros.	NO	No aplica, porque en el giro de negocio de la empresa no se realiza desarrollo de sistemas.
A.14.2.6	Ambiente de desarrollo seguro.	NO	No aplica, porque en el giro de negocio de la empresa no se realiza desarrollo de sistemas.
A.14.2.7	Desarrollo externalizado.	NO	No aplica, porque en el giro de negocio de la empresa no se realiza desarrollo de sistemas.
A.14.2.8	Pruebas de seguridad del sistema.	NO	No aplica, porque en el giro de negocio de la empresa no se realiza desarrollo de sistemas.
A.14.2.9	Pruebas de aceptación de sistemas.	NO	No aplica, porque en el giro de negocio de la empresa no se realiza desarrollo de sistemas.
A.14.3 Datos de prueba			
A.14.3.1	Protección de los datos de prueba.	NO	No aplica, porque en el giro de negocio de la empresa no se realiza desarrollo de sistemas.

Tabla 2.58. Documento de aplicabilidad relacionado a las relaciones con proveedores

A.15 RELACIONES CON PROVEEDORES			
CONTROL		**APLICA**	**OBSERVACIONES**
A.15.1 Seguridad de la información en relación con los proveedores			
A.15.1.1	Política de seguridad de la información en las relaciones con los proveedores.	NO	No aplica, porque en el giro de negocio de la empresa no se realiza desarrollo de sistemas.
A.15.1.2	Requisitos de seguridad en contratos con terceros.	NO	No aplica, porque en el giro de negocio de la empresa no se realiza desarrollo de sistemas.
A.15.1.3	Cadena de suministro de tecnologías de la información y de las comunicaciones.	NO	No aplica, porque en el giro de negocio de la empresa no se realiza desarrollo de sistemas.
A.15.2 Gestión de la provisión de servicios del proveedor			
A.15.2.1	Monitoreo y revisión de los servicios de proveedores.	NO	No aplica, porque en el giro de negocio de la empresa no se realiza desarrollo de sistemas.
A.15.2.2	Gestión de cambios en los servicios de proveedores.	NO	No aplica, porque en el giro de negocio de la empresa no se realiza desarrollo de sistemas.

Tabla 2.59. Documento de aplicabilidad relacionado a la gestión de incidentes de seguridad de la información.

A.16 GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN			
CONTROL		**APLICA**	**OBSERVACIONES**
A.16.1 Gestión de incidentes de seguridad de la información y mejoras			
A.16.1.1	Responsabilidades y procedimientos.	SI	Aplica porque este control está incluido en el alcance del SGSI.
A.16.1.2	Informe de los eventos de seguridad de la información.	SI	Aplica porque este control está incluido en el alcance del SGSI.
A.16.1.3	Informe de debilidades de seguridad de la información.	SI	Aplica porque este control está incluido en el alcance del SGSI.
A.16.1.4	Apreciación y decisión sobre los eventos de seguridad de la información.	SI	Aplica porque este control está incluido en el alcance del SGSI.
A.16.1.5	Respuesta a incidentes de seguridad de la información.	SI	Aplica porque este control está incluido en el alcance del SGSI.
A.16.1.6	Aprendizaje de los incidentes de seguridad de la información.	SI	Aplica porque este control está incluido en el alcance del SGSI.
A.16.1.7	Recopilación de evidencias.	SI	Aplica porque este control está incluido en el alcance del SGSI.

Tabla 2.60. Documento de aplicabilidad relacionado a los aspectos de seguridad de la información para la gestión de la continuidad del negocio

A.17 ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN PARA LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO			
CONTROL		**APLICA**	**OBSERVACIONES**
A.17.1 Continuidad de seguridad de la información			
A.17.1.1	Planificación de la continuidad de la seguridad de la información.	SI	Aplica porque este control está incluido en el alcance del SGSI.
A.17.1.2	Implementación de la continuidad de seguridad de la información.	SI	Aplica porque este control está incluido en el alcance del SGSI.
A.17.1.3	Verificar, revisar y evaluar la continuidad de seguridad de la información.	SI	Aplica porque este control está incluido en el alcance del SGSI.
A.17.2 Redundancias			
A.17.2.1	Disponibilidad de las instalaciones de procesamiento de la información.	SI	Aplica porque este control está incluido en el alcance del SGSI.

Tabla 2.61. Documento de aplicabilidad relacionado al cumplimiento

A.18 CUMPLIMIENTO			
CONTROL		**APLICA**	**OBSERVACIONES**
A.18.1 Cumplimiento de los requisitos legales y contractuales			
A.18.1.1	Identificación de la legislación aplicable y de los requisitos contractuales.	NO	No aplica, porque está fuera del alcance del SGSI.
A.18.1.2	Derechos de propiedad intelectual.	SI	Si, aplica porque este control está incluido en el alcance del SGSI.
A.18.1.3	Protección de los registros.	NO	No aplica, porque está fuera del alcance del SGSI.
A.18.1.4	Protección y privacidad de la información de carácter personal.	NO	No aplica, porque está fuera del alcance del SGSI.
A.18.1.5	Reglamentos de controles criptográficos.	NO	No aplica, porque está fuera del alcance del SGSI.
A.18.2 Revisiones de seguridad de la información			
A.18.2.1	Revisión independiente de la seguridad de la información.	NO	No aplica, porque está fuera del alcance del SGSI.
A.18.2.2	Cumplimiento de las políticas y normas de seguridad.	NO	No aplica, porque está fuera del alcance del SGSI.
A.18.2.3	Comprobación del cumplimiento.	NO	No aplica, porque está fuera del alcance del SGSI.

2.3.1.7. Selección de los Controles Establecidos

Una vez realizado el Documento de Aplicabilidad (SoA) se seleccionarán los controles en función de las amenazas correspondientes a cada activo, que permitan contrarrestar el Riesgo Actual que presenten los activos. El conjunto de controles seleccionados disminuirá el Riesgo Actual que presentan las amenazas identificadas para cada activo.

2.3.1.8. Evaluación del Grado de Madurez o Eficacia de los Controles

La evaluación del grado de madurez de los controles existentes será de gran utilidad para la obtención del Riesgo Actual, así también la evaluación en los controles establecidos permitirá determinar el Riesgo Planificado.

- **NIVEL DE MADUREZ DE LOS CONTROLES EXISTENTES**

Para la evaluación del grado de madurez de los controles existentes se utiliza la **Tabla 2.32.** Escala de valoración de la eficacia del control existente; una vez seleccionados los controles del documento de aplicabilidad se realiza una breve comparación con los controles que ya existen en la empresa. Para esta valoración únicamente se consideró el criterio del jefe del área de TI.

Ejemplo: Nivel de Madurez de los Controles Existentes

Activo de Información: Base de datos de clientes y proveedores

Amenaza: Errores de los usuarios

Riesgo Potencial: Valor 4 y nivel de criticidad alto

Controles:

Los controles seleccionados, en función al documento de aplicabilidad al tipo de amenazas y al riesgo que podrían reducir el riesgo de que se produzcan errores de usuarios, son los siguientes:

- 5.1.1 Políticas para la seguridad de la información.
- 6.1.1 Roles y responsabilidades de seguridad de la información.
- 9.1.1 Política de control de accesos.
- 13.2.1 Políticas y procedimientos de transferencia de información.
- 13.2.4 Acuerdos de confidencialidad o no revelación.
- 17.1.1 Planificación de la continuidad de la seguridad de la información.

Se realiza una breve comparación con los controles existentes en la empresa; se determina que cuenta únicamente con los siguientes controles:

- 6.1.1 Roles y responsabilidades de seguridad de la información.
- 9.1.1 Política de control de accesos.

Por lo tanto, el nivel de madurez evaluado según los criterios de la **Tabla 2.32.** Escala de valoración de la eficacia del control existente, indica que para este caso es de valor **L1** como se indica en la **Tabla 2.63**, valor que representa el 20% de madurez de los controles 6.1.1 y 9.1.1, es decir que está en una etapa inicial y técnicamente no está bien definido para enfrentar o contrarrestar los riesgos que se pueden generar a causa de los errores de usuarios, además sus procedimientos no son muy claros para su uso normal y en caso de incidencias.

- **NIVEL DE MADUREZ DE LOS CONTROLES ESTABLECIDOS**

Para la evaluación del grado de madurez de los controles establecidos se fija un lapso de 1 año en el que podrían implementarse dichos controles; por lo tanto, se evalúa en función de ese criterio, el Riesgo Actual y las valoraciones indicadas en la **Tabla 2.32**.

Ejemplo:

Activo de Información: Base de datos de clientes y proveedores

Amenaza: Errores de los usuarios

Riesgo Potencial: Valor 4 y nivel de criticidad alto (Ver la **Tabla 2.47.** Valoración del Riesgo Potencial [INFO_PER]).

Riesgo Actual: Valor 3 y nivel de criticidad moderado (Ver la **Tabla 2.63.** Matriz de Gestión de Riesgos Actual y Planificado: [INFO_PER]).

Controles:

Los controles establecidos para contrarrestar el riesgo que puede ocasionar una amenaza han sido seleccionados en función del criterio del Jefe de TI, los mismos que pueden variar según la funcionalidad, tipo y costo del activo. A continuación, se listan los controles seleccionados:

- 5.1.1 Políticas para la seguridad de la información.
- 6.1.1 Roles y responsabilidades de seguridad de la información.
- 9.1.1 Política de control de accesos.

- 13.2.1 Políticas y procedimientos de transferencia de información.
- 13.2.4 Acuerdos de confidencialidad o no revelación.
- 17.1.1 Planificación de la continuidad de la seguridad de la información.

El nivel de madurez de los controles seleccionados para contrarrestar el Riesgo Actual generado a causa de los errores de usuarios es **L2,** con un 40% de madurez el control ya es reproducible, pero intuitivo, técnicamente tiene un nivel de definición moderado para enfrentar los riesgos que protege y sus procedimientos están claros para el uso normal y en caso de incidencias. Esto indica que en el lapso de 1 año el Riesgo Actual disminuiría en 2 puntos; y de esta manera se obtendría un Riesgo Planificado muy bajo de valor 1 como se indica en la **Tabla 2.63.** Matriz de Gestión de Riesgos Actual y Planificado: [INFO_PER].

2.3.1.9. Análisis del Riesgo Actual

El Riesgo Actual se lo obtiene en función del Riesgo Potencial y los controles existentes; para su evaluación se hace uso de la valoración por niveles de madurez de los controles que se indica en la **Tabla 2.32.** Escala de valoración de la eficacia del control existente. Una vez obtenido este nivel de madurez en los controles existentes, se evalúan los puntos que disminuirían en el Riesgo Actual, es decir, si el nivel de madurez es **L0**, el Riesgo Actual sería igual al Riesgo Planificado y si el nivel de madurez es **L1 o mayor** los puntos que van a disminuir son más altos y disminuiría notablemente el Riesgo Actual.

Este análisis se lo hizo con la colaboración del Jefe de TI quien proveía de la información referente a los controles existentes.

Ejemplo: Análisis de Riesgo Actual

Activo de Información: Base de datos de clientes y proveedores

Amenaza: Errores de los usuarios

Riesgo Potencial: Valor 4 y nivel de criticidad alto

Controles Existentes: Ver la **Tabla 2.63.** Matriz de Gestión de Riesgos Actual y Planificado: [INFO_PER].

Nivel de Madurez: L1

Puntos: 1

Riesgo Actual:

El Riesgo Actual del activo de la base de datos de clientes y proveedores en función de una de las amenazas corresponde a errores de usuarios en moderado con un valor 3 como se indica en la **Tabla 2.63.** Matriz de Gestión de Riesgos Actual y Planificado: [INFO_PER]. Este cálculo fue realizado tomando en cuenta el valor de cada dimensión del Riesgo Potencial y mediante la disminución de puntos correspondientes al nivel de madurez.

2.3.1.10. Aceptación y tratamiento del Riesgo Actual

En la **Tabla 2.62** se muestra la matriz de tratamiento del riesgo para el activo base de datos de clientes y proveedores, la misma que parte de los criterios definidos en la **Tabla 2.33.** Criterios de Aceptación y Tratamiento del Riesgo .

En el siguiente ejemplo se realiza el análisis de los resultados obtenidos en la matriz de tratamiento del riesgo correspondiente al activo base de datos de clientes y proveedores.

Ejemplo: Aceptación y tratamiento del riesgo

Activo de Información: Base de datos de clientes y proveedores

Amenaza: Errores de los usuarios

Riesgo Actual: Valor 3 y nivel de criticidad moderado

Tratamiento del Riesgo:

El Riesgo Actual tiene un nivel moderado, entonces según el criterio de aceptación se debe reducir el riesgo, mediante la implementación de los controles seleccionados y el nivel de madurez del control en el intervalo de tiempo que se lo ha planificado, es decir, que en 1 año de implementación de los controles se podría observar si efectivamente se redujo el riesgo.

- **INFORMACIÓN: [INFO_PER]**

Tabla 2.62. Matriz de tratamiento del riesgo [INFO_PER]

[INFO] INFORMACIÓN					
[INFO_PER]	**Base de datos de clientes y proveedores**				
AMENAZAS	**RIESGO ACTUAL**		**TRATAMIENTO DEL RIESGO**	**CONTROLES/ SALVAGUARDAS SELECCIONADOS ***	
	Rt	**NIVEL**	**NIVEL**		
5.3.1. [E.1] Errores de los usuarios	3	MODERADO	REDUCIR EL RIESGO	5.1.1	Políticas para la seguridad de la información.
5.3.2. [E.2] Errores del administrador	4	ALTO	REDUCIR EL RIESGO	6.1.1	Roles y responsabilidades de seguridad de la información.
5.3.10. [E.15] Alteración accidental de la información	3	MODERADO	REDUCIR EL RIESGO	8.2.1	Clasificación de la información.
5.3.11. [E.18] Destrucción de información	3	MODERADO	REDUCIR EL RIESGO	9.1.1	Política de control de accesos.
5.3.12. [E.19] Fugas de información	4	ALTO	REDUCIR EL RIESGO	13.2.1	Políticas y procedimientos de transferencia de información.
5.4.3. [A.5] Suplantación de la identidad del usuario	3	MODERADO	REDUCIR EL RIESGO	13.2.4	Acuerdos de confidencialidad o no revelación.
5.4.4. [A.6] Abuso de privilegios de acceso	1	MUY BAJO	ACEPTAR EL RIESGO	16.1.5	Respuesta a incidentes de seguridad de la información.
5.4.9. [A.11] Acceso no autorizado	2	BAJO	ACEPTAR EL RIESGO	12.1.2	Gestión de cambios.
5.4.13. [A.15] Modificación deliberada de la información	1	MUY BAJO	ACEPTAR EL RIESGO	17.1.1	Planificación de la continuidad de la seguridad de la información.
5.4.15. [A.19] Divulgación de información	3	MODERADO	REDUCIR EL RIESGO	18.1.2	Derechos de propiedad intelectual.

En el **ANEXO H**, se muestra la matriz completa del tratamiento de riesgos en cada activo, donde se indican las amenazas, el Riesgo Actual obtenido, su respectivo nivel de aceptación y los controles seleccionados, el tratamiento del riesgo se lo efectúa una vez

que se ponga en marcha el proyecto desarrollado en la empresa, consecuentemente se podría obtener los resultados reales del Riesgo Planificado.

En este proyecto se realiza también el análisis del Riesgo Planificado, bajo proyecciones supuestas en las que se indica que el proyecto será implementado durante un intervalo de tiempo.

2.3.1.11. Análisis del Riesgo Planificado

Para el análisis se considera la aceptación y el tratamiento del Riesgo Actual y se establece que, en el lapso de 1 año, los controles establecidos deben estar en desarrollo o implementación, por lo cual se estima que disminuirá el riesgo en 1 o 2 puntos dependiendo del tipo de amenazas.

El Riesgo Planificado se obtendrá en función del tipo de tratamiento del Riesgo Actual y de los controles seleccionados; su resultado tendrá valoraciones menores que el Riesgo Actual como se muestra en la **Tabla 2.63.** Matriz de Gestión de Riesgos Actual y Planificado: [INFO_PER], adjuntada en el **ANEXO I.**

Ejemplo: Análisis del Riesgo Planificado

Activo de Información: Base de datos de clientes y proveedores

Amenaza: Errores de los usuarios

Riesgo Potencial: Valor 4 y nivel de criticidad alto

Controles Existentes: (Ver la **Tabla 2.63.** Matriz de Gestión de Riesgos Actual y Planificado: [INFO_PER].

Nivel de Madurez: L1

Puntos: 1

Riesgo Actual: Valor 3 y nivel de criticidad moderado

Aceptación y tratamiento del riesgo: Debido a que el nivel de criticidad del riesgo es moderado, se establece que dicho riesgo se debe reducir.

Riesgo Planificado

El Riesgo Planificado del activo de la base de datos de clientes y proveedores es de valor 1 con un nivel muy bajo como se indica en la **Tabla I.2.** Matriz de Gestión de Riesgos Actual y Planificado: [INFO_PER], es decir, que en 1 año de implementación de los controles se podría observar una madurez notable en los controles. Para la obtención del Riesgo

Planificado se tiene que el nivel de madurez del control seleccionado es **L2,** lo que indica la disminución de dos puntos del Riesgo Actual.

2.3.3. MATRIZ DE GESTIÓN DE RIESGOS POTENCIAL, ACTUAL Y PLANIFICADO

Una vez efectuada la metodología de análisis y gestión de riesgos se obtiene la matriz general de gestión de riesgos, en la que se muestra a detalle todos los resultados obtenidos en cada activo.

En el **ANEXO I** se muestran las tablas a detalle (ver desde la **Tabla I.1** hasta la **Tabla I.42**) y para este análisis en la **Tabla I.2** se indica la matriz de riesgos correspondiente al activo base de datos de clientes y proveedores, en base al cual se ha realizado el análisis paso a paso de cálculos y valoración correspondientes a la metodología aplicada.

En esta matriz se puede visualizar que el Riesgo Potencial crítico o muy alto es a causa de los errores del administrador y para el cálculo del Riesgo Actual de la empresa se verifico que existen controles que disminuyen el riesgo en un punto y éste pasa a ser de un nivel 5 (muy alto) a un valor 4 (alto). En consecuencia, de esto y una vez realizado el tratamiento del riesgo se establece que se debe disminuir el riesgo, a través de la implementación de los controles seleccionados, lo que permitirá obtener un Riesgo Planificado mucho menor e igual a 2 (bajo).

- **INFORMACIÓN: [INFO_PER]**

Tabla 2.63. Matriz de Gestión de Riesgos Actual y Planificado: [INFO_PER]

[INFO] INFORMACIÓN																									
[INFO_PER]	Base de datos de clientes y proveedores																								
AMENAZAS	RIESGO POTENCIAL					CONTROLES/ SALVAGUARDAS EXISTENTES	NIVEL DE MADUREZ - CONTROLES EXISTENTES		RIESGO ACTUAL					CONTROLES/ SALVAGUARDAS SELECCIONADOS			NIVEL DE MADUREZ - CONTROLES ESTABLECIDOS		RIESGO PLANIFICADO					
	RIESGO POTENCIAL POR DIMENSIONES			RIESGO POTENCIAL TOTAL					RIESGO POR DIMENSIONES			RIESGO ACTUAL TOTAL							RIESGO POR DIMENSIONES			RIESGO TOTAL	
	Ri	Rc	Rd	Rt	NIVEL		NIVEL	PUNTOS	Ri	Rc	Rd	Rt	NIVEL				NIVEL	PUNTOS	Ri	Rc	Rd	Rt	NIVEL
5.3.1. [E.1] Errores de los usuarios	4	4	4	4	ALTO	Existen controles para la gestión de acceso, donde los usuarios tienen perfiles diferentes según los roles y responsabilidades. Existen controles de acuerdos de confidencialidad, para una parte de la información confidencial. No existen controles para la destrucción, fugas y alteración de la información .	L1	1	3	3	3	3	MODERADO	5.1.1	Políticas para la seguridad de la información.	L2	2	1	1	1	1	MUY BAJO
5.3.2. [E.2] Errores del administrador	5	5	5	5	MUY ALTO		L1	1	4	4	4	4	ALTO	6.1.1	Roles y responsabilidades de seguridad de la información.	L2	2	2	2	2	2	BAJO
5.3.10. [E.15] Alteración accidental de la información	3	3	3	3	MODERADO		L0	0	3	3	3	3	MODERADO	8.2.1	Clasificación de la información.	L1	1	2	2	2	2	BAJO
5.3.11. [E.18] Destrucción de información	2	3	3	3	MODERADO		L0	0	2	3	3	3	MODERADO	9.1.1	Política de control de accesos.	L1	1	1	2	2	2	BAJO
5.3.12. [E.19] Fugas de información	4	4	4	4	ALTO		L0	0	4	4	4	4	ALTO	13.2.1	Políticas y procedimientos de transferencia de información.	L2	2	2	2	2	2	BAJO
5.4.3. [A.5] Suplantación de la identidad del usuario	3	3	1	3	MODERADO		L0	0	3	3	1	3	MODERADO	13.2.4	Acuerdos de confidencialidad o no revelación.	L2	2	1	1	1	1	MUY BAJO
5.4.4. [A.6] Abuso de privilegios de acceso	2	2	2	2	BAJO		L2	2	1	1	1	1	MUY BAJO	16.1.5	Respuesta a incidentes de seguridad de la información.	L3	3	1	1	1	1	MUY BAJO
5.4.9. [A.11] Acceso no autorizado	3	3	2	3	MODERADO		L1	1	2	2	1	2	BAJO	12.1.2	Gestión de cambios.	L3	3	1	1	1	1	MUY BAJO
5.4.13. [A.15] Modificación deliberada de la información	2	2	1	2	BAJO		L2	2	1	1	1	1	MUY BAJO	17.1.1	Planificación de la continuidad de la seguridad de la información.	L3	3	1	1	1	1	MUY BAJO
5.4.15. [A.19] Divulgación de información	4	4	1	3	MODERADO		L1	1	3	3	1	3	MODERADO	18.1.2	Derechos de propiedad intelectual.	L2	2	1	1	1	1	MUY BAJO

3. RESULTADOS Y DISCUSIÓN

3.1. RESULTADOS

Una vez realizado el diseño del Sistema de Gestión de la Seguridad de la Información para la empresa Curtiembre Quisapincha, se expone de manera resumida el proceso general que considera el diseño.

De la identificación y clasificación de los activos de información, se determina un inventario de 36 activos clasificados según el catálogo de activos del Libro II de MAGERIT v.3, que se hace uso durante el análisis, evaluación y tratamiento del riesgo.

Tabla 3.1. Inventario de Activos de Información

INVENTARIO DE ACTIVOS DE INFORMACIÓN	
TIPOS DE ACTIVOS	**CANTIDAD**
[INFO] Información	**3**
[D] Datos e Información Complementaria	**2**
[K] Claves Criptográficas	**2**
[S] Servicios	**2**
[Sw] Software- Aplicaciones Informáticas	**13**
[Hw] Hardware- Equipos Informáticos	**7**
[Com] Redes de Comunicaciones	**4**
[Aux] Equipo Auxiliar	**3**
TOTAL DE ACTIVOS	**36**

En la **Tabla 3.1** se muestra a detalle la cantidad de activos por cada tipo. A continuación, se realiza una breve descripción de cada tipo de activo.

- [INFO] Información. - Se refiere a toda la información esencial de la empresa. Los 3 activos que constituyen este grupo son: las bases de datos de los sistemas contables, los registros confidenciales como patentes de formulaciones químicas, diseños y registros de marca; y los permisos de funcionamiento, en este caso un permiso esencial es la licencia ambiental vigente para que la empresa pueda operar.
- [D] Datos e Información Complementaria. - Es la información complementaria, que se encuentra almacenada en los servidores y en la nube. Los 2 activos que se incluyen en este grupo son: los *logs* y las copias de seguridad de los registros y datos de la empresa.
- [K] Claves Criptográficas. - Es la información que controla un algoritmo de criptografía (cifrado o codificado). Los 2 activos que pertenecen a este grupo son: los certificados digitales del sitio web y el *token* digital que contienen información confidencial con claves y firmas electrónicas de la empresa.

- [S] Servicios. - Es un conjunto de soluciones que permiten solventar necesidades externas e internas de los sistemas informáticos de la empresa. Los 2 activos que pertenecen a este grupo son: el servicio contable y el servicio web que posee la empresa.
- [Sw] Software - Aplicaciones Informáticas. – Es un conjunto de servicios informáticos que permiten la automatización de procesos y la gestión de la información. Los 13 activos que conforman este grupo son los servidores: OwnCloud, FTP, DNS, Digital Ocean, NGINX, Oracle XE 18c, MySQL 8.0 y Postgresql 13; Google Drive, Microsoft Office Professional 2019, Avast Free Antivirus, Windows/Linux y Proxmox.
- [Hw] Hardware - Equipos Informáticos. – Es un conjunto de equipos físicos, que permiten estructurar la red interna, la conectividad entre servicios y la transferencia de información. Los 7 activos que pertenecen a este grupo son: el servidor físico HP Proliant DL 360P, las computadoras de escritorio, las computadoras Portátiles, los teléfonos móviles, las impresoras, el Switch TP-LINK y el Punto de Acceso.
- [Com] Redes de Comunicaciones. – Es un conjunto de medios de transmisión que permiten el intercambio de información. Los 4 activos que se incluye en este grupo son: la red Inalámbrica, la telefonía móvil, la red local y la fibra óptica del Internet.
- [Aux] Equipo Auxiliar. - Es un grupo de equipos físicos que sirven de soporte y medio de transmisión de la información. Los 3 activos relacionados con este grupo son: el sistema de alimentación interrumpida, el sistema de video vigilancia y el cableado estructurado.

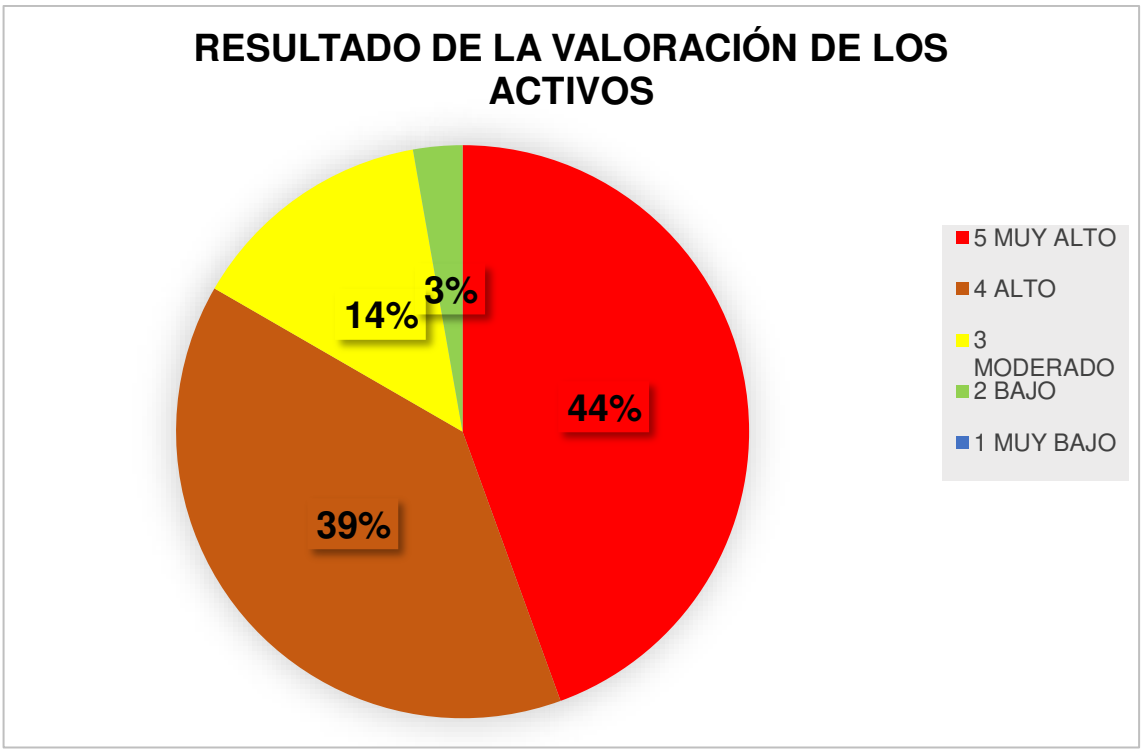


Figura 3.1. Resultados de la valoración de los activos

De la valoración del inventario de activos, se determinó que el costo del activo representa el costo de reposición y el costo del daño económico. El valor de cada activo es resultado de la suma del costo del activo más el costo por dimensiones; el costo por dimensiones se obtuvo a partir del costo valorado en las tres dimensiones estudiadas: Integridad, Confidencialidad y Disponibilidad.

En base a los anterior, se obtuvieron los resultados que se muestran en el diagrama de pastel de la **Figura 3.1**. Aquí se definen los porcentajes que representan cada uno de los activos en los niveles de valoración correspondientes que se describen a continuación:

- MUY ALTO: Representa el 44% del total de activos (16 de 36 activos). Tienen relevancia crítica en la seguridad de la información, es decir, si uno de estos activos sufre daño o pérdida, la empresa se vería afectada de forma grave y podría causar grandes pérdidas económicas.
- ALTO: Representa el 39% del total de activos (14 de 36 activos). Tienen relevancia importante en la seguridad de la información, es decir, si uno de estos activos sufre daño o pérdida, la empresa se vería afectada de forma significativa y podría causar altas pérdidas económicas.
- MODERADO: Representa el 14% del total de activos (5 de 36 activos). Tienen relevancia media en la seguridad de la información, es decir, si uno de estos activos sufre daño o pérdida, la empresa no se vería afectada de forma significativa y no causaría pérdidas económicas importantes.
- BAJO: Representa el 3% del total de activos (1 de 36 activos). Tiene relevancia baja en la seguridad de la información, es decir, si sufre daño o pérdida, la empresa no se vería afectada y no causaría pérdidas económicas.
- MUY BAJO: Representa el 0% del total de activos; no existen activos con valores muy bajos en el inventario de la empresa.

De la identificación de amenazas se realizó un resumen de la cantidad de activos asociados a cada amenaza. En la **Figura 3.2** se observa que el acceso no autorizado es la amenaza común que afecta al 97% de los activos (35 de 36 activos); para disminuir dicha cantidad se deben establecer politicas de control de acceso y trabajar con prioridad en el análisis, gestión y tratamiento del riesgo de dicha amenaza.

Figura 3.2. Activos comunes en cada amenaza

Así también, se obtuvieron que los errores del administrador, abuso de privilegios de acceso, suplantación de la identidad de usuario, averías de origen físico o lógico, errores de los usuarios, destrucción de la información, fugas de información, modificación deliberada de la información y divulgación de la información son amenazas comunes que afectan a más del 50% de los activos de la empresa; por lo que se puede concluir que se deben establecer políticas y procedimientos que contrarresten el riesgo que presentan dichas amenazas.

Para el análisis de los resultados de los riesgos obtenidos se realizó el cálculo de todos los riesgos identificados, son 395 riesgos que se consideraron en este estudio y se los evalúa en función de distintas condiciones, tal como se muestra a continuación.

El Riesgo Potencial es un factor de suma importancia que permite medir el riesgo real en la fase inicial. Considerando que la empresa Curtiembre Quisapincha no tiene implementado ningún control, en función de la seguridad de la información y una vez realizado el análisis de impacto y probabilidades se obtuvo una matriz de riesgos potenciales por activo, de las cuales

se totalizó la cantidad de los riesgos en función de su nivel de criticidad e independientemente del tipo de activo.

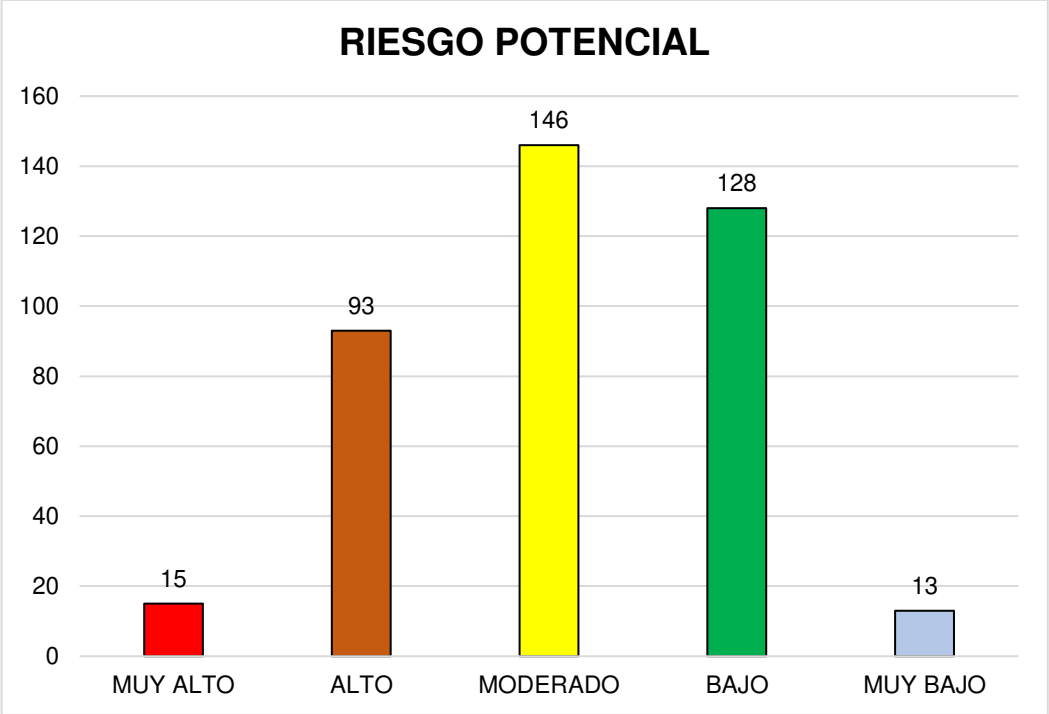


Figura 3.2. Riesgo Potencial Resultante

Se obtuvieron los resultados que se indican en la **Figura 3.2**, en los que se observa que:

- Existen 15 riesgos potenciales en el nivel muy alto que afectarían de forma crítica a varios activos de la empresa en el caso de una amenaza se materialice, pudiendo causar graves daños o pérdidas económicas en la empresa.
- Hay 93 riesgos potenciales con un nivel alto, lo cual implica un gran riesgo en todos los activos de la empresa, pudiendo ocasionar notables pérdidas económicas, por lo tanto, se deberá realizar un tratamiento oportuno de riesgos.
- En el nivel moderado existen 146 riesgos potenciales, es decir, que pueden afectar significativamente a los activos de la empresa, pero sin embargo no se generarían pérdidas económicas graves. Se recomienda realizar el tratamiento de riesgos a tiempo para evitar que el nivel de criticidad incremente en cada uno de estos riesgos.
- Existen 128 riesgos potenciales en el nivel bajo, lo cual indica que los activos relacionados con estos riesgos y amenazas representan un bajo impacto en los objetivos de la empresa.
- En el nivel muy bajo se obtuvieron 13 riesgos potenciales que tienen relevancia insignificante para el giro de negocio de la empresa; así también se puede decir que las amenazas relacionadas no generan mayor impacto y la probabilidad de que ocurra es muy baja.

Cabe resaltar que un activo puede tener a la vez varios riesgos potenciales obtenidos en función de cada amenaza identificada; por lo tanto, los niveles de criticidad de dichos riesgos serán diferentes en cada activo, es decir que el impacto y probabilidad de las amenazas sobre dicho activo son variables y dependen del valor del activo como consecuencia del costo por reposición del activo y el daño económico que este pueda generar en la empresa.

El Riesgo Actual permitió evaluar el riesgo de los activos en las condiciones reales de la empresa Curtiembre Quisapincha, donde se consideran los controles existentes relacionados a cada activo, así también se mide el nivel de madurez de estos para así determinar la cantidad de riesgos actuales que posee la empresa.

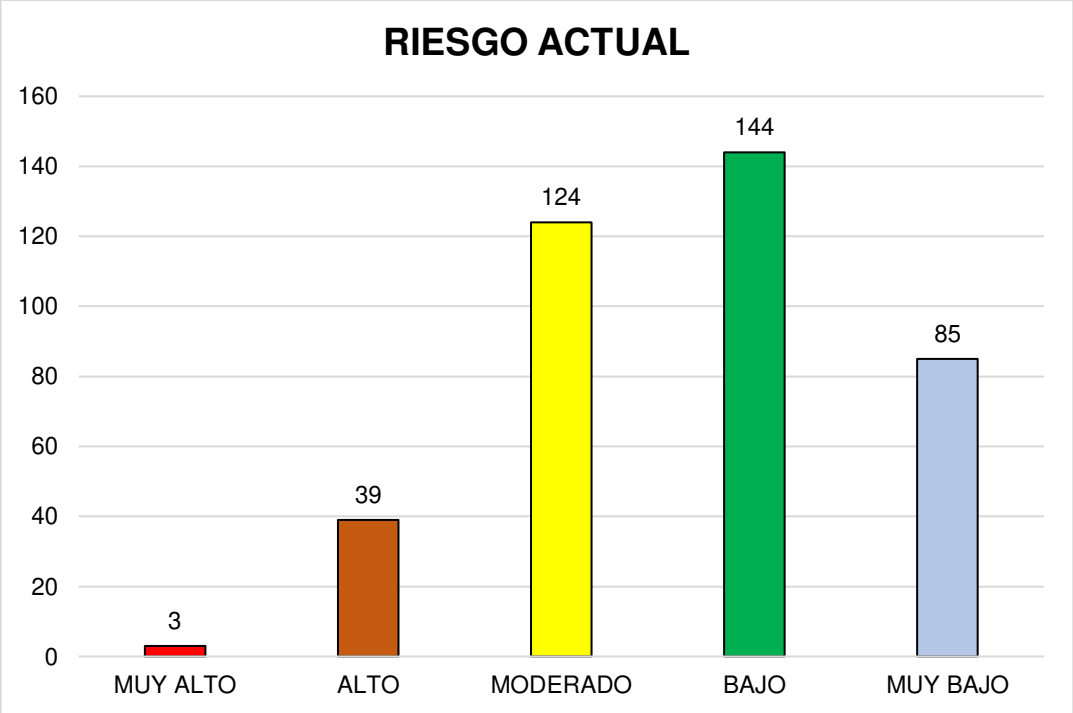


Figura 3.3. Riesgo Actual Resultante

En la **Figura 3.3** se resumen todos los riesgos actuales que afectan a los activos indicados en el inventario y considerados de mayor importancia para la empresa. A continuación, se realiza un breve análisis de estos resultados.

- Existen 3 riesgos actuales que afectan a algunos activos de la empresa; en función de Riesgo Potencial se puede determinar que la empresa cuenta con controles que permiten reducir el Riesgo Potencial, de tal manera que los activos no se verían gravemente afectados.
- Existen 39 riesgos en el nivel alto y que están relacionados con muchos activos de la empresa; y en comparación con los 93 riesgos potenciales hallados inicialmente, se puede apreciar que esta cantidad disminuye notablemente al considerar las condiciones reales de la empresa. En consecuencia, se recomienda realizar una

revisión de los controles existentes, pues estos podrían mejorar y reducir aún más los riesgos potenciales que pudieran tener los activos.

- En el nivel moderado existen 124 riesgos, en el nivel bajo se identificaron 144 riesgos y en el nivel muy bajo hay 85 riesgos; mismos que se los puede reducir realizando un tratamiento adecuado de riesgos.

Se proyecta que este diseño será implementado en la empresa Curtiembre Quisapincha y se realiza el Análisis del Riesgo Planificado en el caso hipotético de que se implanten y cumplan los controles y políticas establecidas para disminuir y aceptar los riesgos actuales.

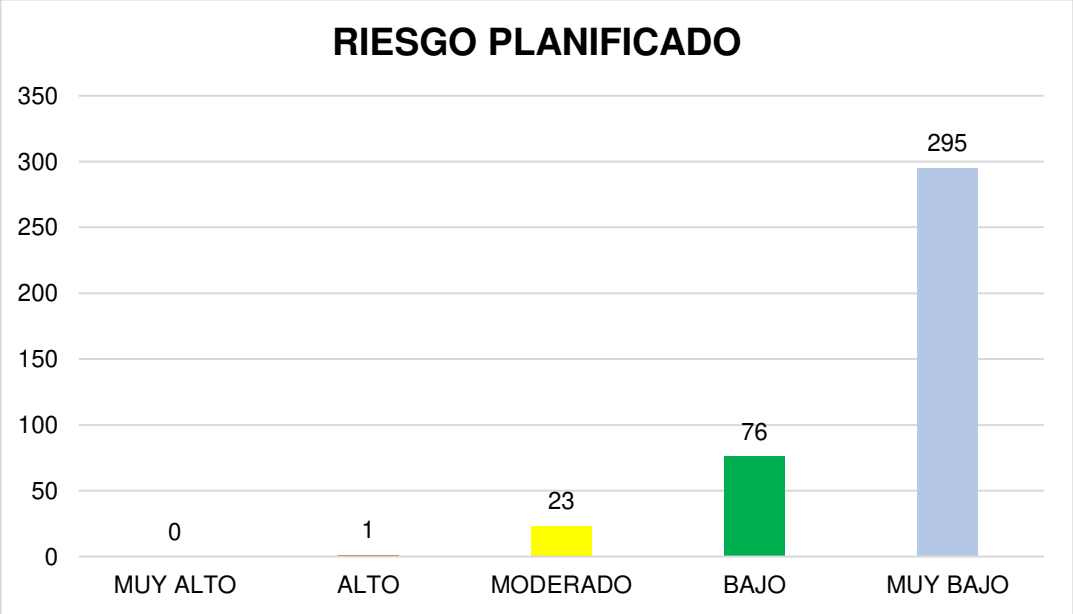


Figura 3.4. Riesgo Planificado Resultante

El Riesgo Planificado representa al resultado del tratamiento del Riesgo Actual en un intervalo de tiempo; en este caso hipotético se consideró un año para volver a realizar la evaluación del riesgo, mismo que representará al Riesgo Planificado.

En la **Figura 3.4** se puede determinar que efectivamente al implementar y ejecutar el SGSI de manera adecuada, cumpliendo las políticas y mejorando continuamente los controles, se pueden reducir notablemente los riesgos actuales de la empresa; se observa que:

- En el nivel muy alto ya no existen riesgos que puedan afectar a los activos, en el nivel alto únicamente existe un riesgo que podría afectar a un activo.
- En el nivel moderado existen 23 riesgos que estarían sujetos a un nuevo tratamiento de riesgos en un nuevo intervalo de tiempo, pudiendo así disminuir su cantidad.
- En el nivel bajo existen 76 riesgos que podrían afectar a los activos de la empresa, estando también sujetos a un nuevo tratamiento de riesgos para disminuir su número.

- Finalmente, se determina que en el nivel muy bajo existe la mayor cantidad de riesgos de todos los niveles, pudiendo notarse que son 295 los riesgos que podrían afectar de forma insignificante a los activos y en consecuencia al giro de negocio de la empresa.

3.2. POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

Realizado el Análisis y la Evaluación de riesgos, y en función de los resultados obtenidos para el tratamiento del riesgo, se define una política de seguridad de la información, donde se detallan los dominios incluidos en el alcance del SGSI según establece la norma NTE INEN-ISO/IEC 27002:2013+Cor. 1:2014+Cor. 2: 2015. Los dominios que se detallan en la política son los siguientes:

A.6. Organización de la seguridad de la información
A.8. Gestión de Activos
A.9. Control de acceso
A.10. Criptografía
A.12. Seguridad de las operaciones
A.13. Seguridad en las comunicaciones
A.16. Gestión de incidentes de seguridad de la información
A.17. Aspectos de seguridad de la información para la gestión de la continuidad del negocio
A.18. Cumplimiento

Los dominios excluidos debido al alcance del SGSI son los siguientes:

A.7. Seguridad de Recursos Humanos
A.11. Seguridad Física y Ambiental
A.14. Adquisición, Desarrollo y Mantenimiento del Sistema
A.15. Relaciones con proveedores

A continuación, se define la política de seguridad de la información en función de los objetivos de control y controles seleccionados para reducir el riesgo de cada activo, considerando el alcance y limitación del SGSI para definir el alcance de las políticas.

CURTIEMBRE QUISAPINCHA

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

3.2.1. INTRODUCCIÓN

El presente documento detalla un conjunto de políticas de seguridades de la información que deberán ser implementadas por la alta dirección, con el fin de reducir o mitigar los riesgos existentes en los activos y concientizar al personal de la empresa.

3.2.2. OBJETIVOS

- Establecer políticas y procedimientos según el Anexo A de la norma ISO 27001:2013, que permita garantizar la seguridad a la información de la empresa Curtiembre Quisapincha.
- Fomentar la asignación de roles y responsabilidades para cada área en la empresa.
- Concientizar a la alta dirección y a su equipo de trabajo, sobre la importancia de ejecutar y mantener un sistema de gestión de seguridad de la información para evitar riesgos de seguridad.

3.2.3. RESPONSABILIDADES

El Jefe del Área de Tecnologías de la Información es el responsable de la administración de la seguridad de la información de la empresa, y es quien realizará revisiones periódicas al cumplimiento de las políticas y procedimientos establecidos.

En tanto que, todos los empleados de la empresa Curtiembre Quisapincha serán responsables de cumplir con las políticas y cuidar de la seguridad de la información de la empresa.

GERENCIA DE SEGURIDAD DE LA INFORMACIÓN	DIRECCIÓN GENERAL	GERENCIA DE TECNOLOGÍA
Victoria Camacho Jefe de Seguridad de la Información	Pablo Hidalgo DIRECTOR	Milton Camacho Jefe de TI Curtiembre Quisapincha

3.2.4. POLÍTICAS GENERALES

3.2.4.1. Organización de la seguridad de la información

3.2.4.1.1. Organización interna

- **Roles y responsabilidades de seguridad de la información**

  Los roles y responsabilidades para el Área de Seguridad de la Información se definen de la siguiente manera:

  La Alta Dirección o Gerente General

  - Autorizar el acceso a la información confidencial para la elaboración del SGSI.
  - Aprobar las políticas de seguridad de la información para la empresa.
  - Autorizar la implementación del SGSI.
  - Autorizar los recursos necesarios para la ejecución del SGSI.
  - Verificar el cumplimiento de los controles y políticas de seguridad de la información para la empresa.
  - Supervisar la implementación del diseño del SGSI.

  El Área de Tecnologías de la Información

  - Gestionar incidentes de seguridad.
  - Ejecutar la implantación del SGSI.
  - Proveer de recursos necesarios para el levantamiento de información.
  - Cumplir con los controles y políticas de seguridad establecidas.
  - Delegar a un responsable del proyecto SGSI.
  - Sancionar al personal en el caso de no cumplimiento de las políticas.

- **Separación de funciones**

  Se deben definir las funciones y tareas en su totalidad, para evitar fallos de seguridad de la información dentro del giro del negocio.

  Para esto se establece lo siguiente:

GERENCIA DE SEGURIDAD DE LA INFORMACIÓN	DIRECCIÓN GENERAL	GERENCIA DE TECNOLOGÍA
Victoria Camacho Jefe de Seguridad de la Información	Pablo Hidalgo DIRECTOR	Milton Camacho Jefe de TI Curtiembre Quisapincha

- Concientizar y capacitar al personal sobre temas de seguridades y responsabilidades sobre cada activo de la empresa.
- Generar un manual de procesos de cada área.
- Distribuir el manual de procesos a cada miembro de las áreas de trabajo.
- Verificar el cumplimiento de los procesos establecidos.
- Sancionar en caso de incumplimiento del manual de procesos.

Con la finalidad de separar las funciones se deberá elaborar el manual de procesos y asignar las responsabilidades a cada miembro del equipo.

- **Contacto con las autoridades**

  Se establece que todos los procesos desarrollados por las diferentes áreas de la empresa deben tener el aval y estar bajo el conocimiento de la alta dirección, antes de ser ejecutados o distribuidos.

- **Contacto con grupos de interés especial**

  Se debe establecer al menos una vez al año contacto con grupos profesionales de asesoría en seguridad de la información, que permitan mejorar el conocimiento y las mejores prácticas en seguridades.

- **Gestión de proyectos de seguridad de la información**

  La alta dirección junto con el equipo del Área de Tecnologías de la Información debe definir objetivos claros y concisos de seguridad de la información, con el fin de incluirlos dentro de los objetivos de todos los proyectos que se desarrollen dentro de la empresa.

3.2.4.1.2. Dispositivos móviles y teletrabajo

- **Política de dispositivo móvil**

  Se deben definir políticas para dispositivos móviles donde se incluyan los siguientes aspectos:

  - Definir objetivos de seguridad de la información de los dispositivos móviles.

GERENCIA DE SEGURIDAD DE LA INFORMACIÓN	DIRECCIÓN GENERAL	GERENCIA DE TECNOLOGÍA
Victoria Camacho Jefe de Seguridad de la Información	Pablo Hidalgo DIRECTOR	Milton Camacho Jefe de TI Curtiembre Quisapincha

- Emitir cartas de confidencialidad siempre que exista nuevo personal en el Área de Ventas.
- Firmar un convenio de responsabilidad sobre el uso adecuado del dispositivo.
- Acordar que el dispositivo móvil es de uso exclusivo para la empresa.
- Establecer la confidencialidad de los datos de clientes, imágenes y multimedia distribuida desde el Área de *Marketing* y Publicidad.
- Definir diferentes perfiles de acceso para cada dispositivo móvil.
- Definir contraseñas con caracteres alfanuméricos para la protección de la base de datos de contactos.
- Habilitar la sincronización de las copias de seguridad de las redes sociales y correos electrónicos asignados.
- Generar un sistema de contraseñas o hacer uso de los aplicativos existentes para códigos intermitentes de acceso a la sesión de redes sociales.
- Instalar las aplicaciones autorizadas por el Área de Tecnologías de Información y el Área de *Marketing* y Publicidad.

- **Política de teletrabajo**

  La empresa no cuenta con la modalidad de teletrabajo, por lo tanto, no se definen políticas para este apartado.

3.2.4.2. Gestión de activos

3.2.4.2.1. Responsabilidad de los activos

- **Inventario de activos**

  Se debe mantener un inventario de activos de información, debidamente clasificados en función de su valor, riesgo de pérdida o compromiso.

- **Propiedad de los activos**

  Se deben asignar propietarios autorizados de cada activo, quienes deberán ser responsables del manejo adecuado y de su seguridad.

- **Uso aceptable de los activos**

  Se debe establecer una política que especifique reglas para el uso aceptable de cada activo con su respectivo responsable del uso.

- **Devolución de activos**

  Se debe documentar a detalle la política ya establecida, donde se especifique que se realizará un acta de entrega de los activos y del cargo al finalizar el contrato laboral.

3.2.4.2.2. Clasificación de la información

- **Clasificación**

  Se debe especificar un esquema de clasificación de la información.

  El Área de Tecnologías de Información debe definir dicho esquema en función de los niveles de importancia de la información.

  Todos los empleados de CQ, deben clasificar la información en función de un manual que deberá proveer el Área de Tecnologías de Información.

- **Etiquetado de la información**

  Se debe detallar el procedimiento de etiquetado según el esquema de clasificación de la información.

  Se debe generar un formato de etiquetado de la información, que contenga códigos según el área correspondiente.

- **Manejo de los activos**

  Se deben manejar los activos en función del esquema de clasificación de la información.

  Se debe establecer niveles de importancia de los activos relacionados a la información.

  Se debe elaborar un manual de manejo de activos en función a la seguridad de la información.

  Se debe reportar a todo el personal sobre el manual de manejo de activos.

GERENCIA DE SEGURIDAD DE LA INFORMACIÓN	DIRECCIÓN GENERAL	GERENCIA DE TECNOLOGÍA
Victoria Camacho Jefe de Seguridad de la Información	Pablo Hidalgo DIRECTOR	Milton Camacho Jefe de TI Curtiembre Quisapincha

3.2.4.2.3. Manejo de los medios

- **Gestión de medios extraíbles**

  Se deben implementar políticas y procedimientos para la gestión de medios extraíbles, donde se realice lo siguiente:

  - Usar únicamente los medios extraíbles que provea el Área de Tecnologías de Información.
  - Prohibir el uso de medios extraíbles que no sean de la empresa.
  - Responsabilizarse del medio extraíble asignado.
  - Establecer sanciones económicas en el caso de daño, pérdida o robo del medio extraíble.
  - Firmar un acta de entrega del medio extraíble, para garantizar la recepción y acuerdo entre las partes.

- **Eliminación de los medios**

  Se deben definir los procedimientos a seguir para la eliminación de los medios, pudiendo ser mediante el reseteo del medio extraíble para su reutilización.

- **Transferencia de medios físicos**

  Se debe establecer un proceso de transferencia de medios físicos, en donde el mensajero debe estar autorizado y las empresas proveedoras de mensajería sean seguras y confiables.

  Se debe prohibir el acceso a personal no autorizado en el proceso de mensajería.

3.2.4.3. Control de Acceso

3.2.4.3.1. Requisitos de negocio para el control de acceso

- **Política de control de acceso**

  Se debe definir una política de control de acceso que contenga lo siguiente:

  - Evitar el acceso no autorizado.

- Definir roles y perfiles a cada empleado según las responsabilidades a cargo dentro de la empresa.
- Restringir el acceso una vez finalizada la relación laboral con el empleado.
- Realizar el cambio de contraseñas del perfil de usuario en los sistemas asignados, al menos una vez al mes.
- Cerrar todos los sistemas que contengan el perfil de acceso habilitado.
- Sancionar al personal en el caso de incumplir las políticas de control de acceso.

- **Control de acceso a las redes y servicios asociados**

  Se debe definir una política de control de acceso a redes y servicios de red, que especifiquen los siguiente:

  - Definir un tiempo de autenticación en los aplicativos móviles.
  - Generar un código de seguridad para el acceso a la web, a través de aplicaciones que brinden el servicio de autenticación.
  - Proveer de acceso a la intranet de la empresa.
  - Prohibir la filtración de contraseñas de las redes y servicios al personal no autorizado.
  - Sancionar al personal en el caso de incumplimiento.

3.2.4.3.2. Gestión de acceso de los usuarios

- **Registro y retiro de usuario**

  Se debe documentar la política de registro y retiro de usuario, donde se especifiquen los siguientes puntos:

  - Detallar los perfiles de usuario.
  - Generar credenciales de acceso para los usuarios.
  - Quitar el acceso al personal que haya finalizado su relación laboral con la empresa.
  - Crear perfiles para principiantes.

GERENCIA DE SEGURIDAD DE LA INFORMACIÓN	DIRECCIÓN GENERAL	GERENCIA DE TECNOLOGÍA
Victoria Camacho Jefe de Seguridad de la Información	Pablo Hidalgo DIRECTOR	Milton Camacho Jefe de TI Curtiembre Quisapincha

- **Provisión de acceso a usuarios**

  Se debe documentar la política de provisión de acceso a usuarios, donde se detalle los tipos de acceso a sistemas y servicios, según los perfiles y roles establecidos. Para esto se deberá mantener un registro central de accesos y se eliminarán derechos de acceso a aquellos empleados que dejen la empresa.

- **Gestión de privilegios de derechos de acceso**

  Se debe documentar la política de gestión de privilegios de derechos de acceso, donde se detallen los servicios y sistemas restringidos con su respectivo acceso privilegiado para el usuario que corresponda.

- **Gestión de la información secreta de autenticación de los usuarios**

  Se debe establecer una política donde se especifique que los usuarios deben firmar un compromiso de confidencialidad de la información secreta, así mismo se debe verificar la identidad de cada usuario y su respectivo acceso.

- **Revisión de los derechos de acceso de usuario**

  Se debe documentar la política y establecer un plan de revisiones de los accesos de usuario a intervalos regulares.

- **Retiro y ajuste de los derechos de acceso**

  Se debe documentar la política y establecer un plan de retiro y ajuste de los accesos del empleado cuando finalice su relación laboral con la empresa.

3.2.4.3.3. Responsabilidades del usuario

- **Uso de la información secreta de autenticación**

  Se debe documentar la política de uso de la información secreta de autenticación que contenga lo siguiente:

- Firmar acuerdos de confidencialidad de la información secreta de autenticación.
- Cambiar constantemente la información secreta de autenticación.
- Eliminar el acceso a las personas autorizadas que hayan finalizado el contrato laboral con la empresa.
- Responsabilizar al usuario sobre el uso adecuado de la información secreta de autenticación y sobre el servicio al cual de acceso dicha información.
- Establecer credenciales de autenticación y su nivel de confidencialidad.

3.2.4.3.4. Control de acceso a sistemas y aplicaciones

- **Restricción del acceso a la información**

  Se debe documentar dicho proceso en función de la política de acceso, para garantizar la integridad de la información y las buenas prácticas de seguridades.

- **Procedimientos seguros de inicio de sesión**

  Se debe definir y documentar una política que especifique el procedimiento seguro para el inicio de sesión, propio para la empresa.

- **Sistema de gestión de contraseñas**

  Se debe definir y documentar una política que defina un procedimiento que detalle lo siguiente:

  - Utilizar formatos de contraseñas con un nivel medio- alto de complejidad.
  - Utilizar contraseñas con caracteres alfanuméricos,
  - Evitar la reutilización de contraseñas.
  - Realizar cambios de contraseñas en intervalos definidos.
  - Centralizar la gestión de contraseñas al Área de Tecnologías de Información.
  - Permitir el restablecimiento de perfiles de usuarios cuando estos se hayan bloqueado.
  - Sancionar al personal que incumpla esta política.

GERENCIA DE SEGURIDAD DE LA INFORMACIÓN	DIRECCIÓN GENERAL	GERENCIA DE TECNOLOGÍA
Victoria Camacho Jefe de Seguridad de la Información	Pablo Hidalgo DIRECTOR	Milton Camacho Jefe de TI Curtiembre Quisapincha

3.2.4.4. Criptografía

3.2.4.4.1. Controles criptográficos

- **Política de uso de los controles criptográficos**

  Se debe implementar una política sobre el uso de controles criptográficos para el certificado SSL, el uso de los medios extraíbles y dispositivos móviles.

- **Gestión de Llaves**

  Se debe implementar una política para la gestión de llaves criptográficas, donde se incluya el proceso de generación, almacenamiento, archivo, recuperación, distribución, retiro y destrucción de estas.

3.2.4.5. Seguridad de las operaciones

3.2.4.5.1. Procedimientos y responsabilidades operacionales

- **Documentación de procedimientos de operación**

  Se debe implementar una política donde se establezca lo siguiente:

  - Redactar un manual de procedimientos de operación de las actividades realizadas en cada área de la empresa.
  - Controlar los procedimientos a través de bitácoras.
  - Documentar todos las actividades y procesos de cada área de la empresa.
  - Establecer responsabilidades a una persona que realice el control de la documentación.

- **Gestión de cambios**

  Se debe establecer una política de gestión de cambios, para evidenciar todos los procesos y evitar riesgos en la seguridad de la información.

  Se debe realizar un control de versiones para evitar pérdida de información.

- **Gestión de capacidades**

  Se debe desarrollar una política que especifique la capacidad del sistema de tecnologías de la información para asegurar la funcionalidad del negocio.

- **Separación de ambientes de desarrollo, pruebas y producción**

  Se debe definir una política referente a la separación de ambiente de desarrollo, pruebas y producción, para evitar fallas de seguridad en las bases de datos de la empresa.

  Se debe realizar el *backup* de cada ambiente para respaldar la información en los servidores y en la nube.

3.2.4.5.2. Protección contra un malware

- **Controles contra *malware***

  Se debe proporcionar mecanismos necesarios que garanticen la protección de la información y aplicativos utilizados en toda la infraestructura de red, donde se procesa y almacenan los datos, para mitigar el riesgo de que la información sea divulgada, modificada o eliminada por algún software malicioso o *malware*.

3.2.4.5.3. Copias de seguridad

- **Copias de seguridad de la información**

  Las copias de seguridad de respaldo y almacenamiento de información se realizarán de forma periódica y deben ser notificadas con alertas en el servidor o sistemas que posee la empresa.

3.2.4.5.4. Registro y monitoreo

- **Registro de eventos**

  Se debe establecer un proceso para realizar el monitoreo periódico de los eventos generados en los servidores, bases de datos y sistemas de información.

- **Protección de la información de registro**

  Se debe realizar un monitoreo constante de los sistemas de información que puedan ser susceptibles a incidentes de seguridad. Se debe garantizar la Integridad, Confidencialidad y Disponibilidad de la información, por lo que se debe capacitar al personal para reducir el riesgo.

GERENCIA DE SEGURIDAD DE LA INFORMACIÓN	DIRECCIÓN GENERAL	GERENCIA DE TECNOLOGÍA
Victoria Camacho Jefe de Seguridad de la Información	Pablo Hidalgo DIRECTOR	Milton Camacho Jefe de TI Curtiembre Quisapincha

- **Registros de administración y operación**

  Se deben revisar periódicamente los registros de los usuarios y administrador de los sistemas contable, facturación electrónica y recursos humanos, para evitar fugas de información y reducir el riesgo de posibles brechas de seguridad.

- **Sincronización del reloj**

  Se debe instalar un sistema que sincronice los relojes de los servidores, bases de datos y sistema contable para garantizar el procesamiento adecuado de la información.

3.2.4.5.5. Control del software operacional

- **Instalación del software en los sistemas operativos**

  Se debe asignar a un responsable por parte del Área de Tecnologías de Información para controlar la instalación adecuada, el correcto funcionamiento y actualizaciones en el software y sistemas operativos de todas las áreas.

  Se debe sancionar al personal no autorizado que realice alguna instalación de software en los sistemas operativos.

  El Área de Tecnologías de Información deberá garantizar la funcionalidad de los programas, software, servicios web y sistemas.

  El Área de Tecnologías de Información debe reportar a la Alta Gerencia en el caso de que existan fallos en los sistemas operativos.

3.2.4.5.6. Gestión de la vulnerabilidad técnica y restricción en la instalación del software

- **Gestión de vulnerabilidades técnicas**

  Se debe establecer un procedimiento de gestión de vulnerabilidades técnicas que detalle lo siguiente:

  - Revisar periódicamente si existen vulnerabilidades técnicas de los servidores.
  - Revisar periódicamente si existen vulnerabilidades en las bases de datos y sistema contable.

- Capacitar al personal autorizado sobre los tipos de vulnerabilidades y amenazas que existen para garantizar la seguridad de la información.
- Reportar de inmediato las vulnerabilidades técnicas halladas en el sistema de información.
- Realizar un historial de vulnerabilidades para tener un tiempo de respuesta menor durante la identificación de estos.

- **Restricción en la instalación del software**

  El personal del Área de Tecnologías de la Información es responsable de la instalación del software en todos los dispositivos fijos y móviles de la red, por lo tanto, esta actividad está restringida para usuarios de otras áreas.

3.2.4.5.7. Consideraciones sobre la auditoría de sistemas de información

- **Controles de auditoría de los sistemas de información**

  Se debe realizar un monitoreo continuo para evaluar los procesos según se establece en la política de la organización; además se debe verificar el nivel de implementación, mantenimiento y mejora continua del sistema de seguridad de la información.

3.2.4.6. Seguridad en las comunicaciones

3.2.4.6.1. Gestión de la seguridad de redes

- **Controles de red**

  Se debe establecer un proceso que permita controlar la red, considerando los siguientes puntos importantes:

  - Realizar un monitoreo de los eventos realizados en los equipos de red, con el fin de evitar fallos y fugas de información.
  - Concientizar al personal de la empresa sobre la seguridad en los equipos de la red interna.
  - Manejar perfiles de acceso en la intranet.
  - Restringir el acceso libre a través de la red inalámbrica.

- Gestionar las redes por áreas con sus respectivas funcionalidades.

- **Seguridad de los servicios de red**

  Se debe limitar el acceso a servicios de red que no sean requeridos; además se debe establecer una política de control de acceso donde se tengan perfiles de acceso asignados a los usuarios.

- **Separación en las redes**

  Se debe definir una manual de procedimientos que detalle lo siguiente:

  - Mantener un sistema de cableado estructurado.
  - Establecer una red interna segmentada por dominios y grupos de usuarios para evitar inconsistencias y el acceso a dominios no autorizados.
  - Segregar redes diferentes para cada área de la empresa con el fin de evitar filtración de datos.
  - Mantener perfiles de acceso a cada red.
  - Concientizar y capacitar al personal que vaya a hacer uso de estas redes.
  - Sancionar a los usuarios de la red que incumplan las políticas de control de acceso.

3.2.4.6.2. Transferencia de información

- **Políticas y procedimientos de transferencia de información**

  Se debe establecer un procedimiento para asegurar la protección de la información a ser transferida o enviada a otras empresas, para lo cual se debe utilizar un servicio de correo seguro y cifrado extremo a extremo para evitar filtración de datos.

- **Acuerdos de transferencia de información**

  Se deben definir acuerdos para la transferencia de información dentro y fuera de la empresa; así también, se deben establecer cartas de acuerdos de confidencialidad para empleados, clientes y proveedores que se involucren en el giro de negocio.

- **Mensajería electrónica**

  Se debe redefinir el proceso de mensajería instantánea y establecer que toda información debe ser enviada a través de un correo seguro y cifrado para evitar filtración de datos. Se debe también implementar un servicio de correo interno para cada área de la empresa, con el fin de brindar Integridad, Confidencialidad y Disponibilidad de datos en la red interna de la empresa.

- **Acuerdos de confidencialidad o no revelación**

  Se deben definir acuerdos de confidencialidad para los empleados de la empresa donde se establezcan todos los activos confidenciales que se muestran a continuación:

  - Patentes de formulaciones químicas.
  - Bases de datos de clientes y proveedores
  - Fichas de costos de los productos terminados y materia prima.
  - Inventario de productos controlados por el CONSEP[22]
  - Registros de permisos de funcionamiento.
  - Nóminas de empleados de la empresa.

3.2.4.7. Gestión de incidentes de seguridad de la información

3.2.4.7.1. Gestión de incidentes de seguridad de la información y mejoras

- **Responsabilidades y procedimientos**

  Se debe definir el procedimiento referente a incidentes de seguridad y asignar a un responsable del Área de Tecnologías de la Información, para gestionar o procesar cualquier incidente que ocurra en la empresa.

  Se debe tener personal capacitado que le permita manejar los incidentes de seguridad de la información.

  Se debe capacitar a todo el personal de la empresa, para que estén en la posibilidad de identificar si es o no un incidente de seguridad de la información.

[22]CONSEP: Consejo Nacional de Control de Sustancias Estupefacientes y Psicotrópicas

- **Informe de los eventos de seguridad de la información**

  Se debe presentar informes de todos los eventos ocurridos en los activos que pueden afectar a la seguridad de la información.

  Se debe concientizar al personal sobre los tipos de incidentes y la importancia de reportar al Área de Tecnologías de la Información.

  Se debe tener un historial de informes de cualquier evento que pueda ocasionar un incidente de seguridad.

  Se debe tener un historial de incidentes para mejorar el tiempo de respuesta, si este se repite.

- **Informe de debilidades de seguridad de la información**

  Se debe capacitar al personal en el tema de seguridades de la información, con el fin de que puedan reportar las debilidades del sistema de información, para evitar de que amenazas como divulgación o fuga de información clasificada se materialicen.

- **Apreciación y decisión sobre los eventos de seguridad de la información**

  El Área de Tecnologías de la Información debe monitorear todas las debilidades de los sistemas de información, para establecer controles que permitan disminuir el riesgo.

  Se deben efectuar charlas y talleres prácticos en los que el personal aprenda a tomar decisiones adecuadas ante un evento de seguridad de la información.

- **Respuesta a incidentes de seguridad de la información**

  Todos los empleados de Curtiembre Quisapincha, tienen la responsabilidad de reportar incidentes o posibles incidentes de seguridad de la información al Área de Tecnologías de la Información

  Es deber del Área de Tecnologías de la Información evaluar todos los incidentes de seguridad y reportar a la Alta Dirección aquellos incidentes que sean relevantes.

  El Área de Tecnologías de la Información debe contar con personal calificado para la gestión de incidentes de seguridad de la información.

GERENCIA DE SEGURIDAD DE LA INFORMACIÓN	DIRECCIÓN GENERAL	GERENCIA DE TECNOLOGÍA
Victoria Camacho Jefe de Seguridad de la Información	Pablo Hidalgo DIRECTOR	Milton Camacho Jefe de TI Curtiembre Quisapincha

Se debe realizar una base de conocimientos de incidentes y respuestas, con el fin de reducir el tiempo de respuesta para incidentes futuros.

Se debe definir una matriz de tiempos de respuesta a los incidentes en función de los incidentes ya ocurridos en la empresa.

Se debe priorizar los incidentes según el RTO definido en el análisis de riesgos, por lo tanto, se tiene:

- Si el incidente es fatal, el tiempo de recuperación máximo debe ser menor a 2 horas.
- Si el incidente es grave, el tiempo de recuperación oscilará en el intervalo de 2 a 4 horas.
- Si el incidente es moderado, el tiempo de recuperación podrá tardar 1 día.
- Si el incidente es bajo y muy bajo, el tiempo de recuperación puede tardar de 2 a 5 días.

Se debe definir un esquema de respuesta rápida para evitar la falta de disponibilidad en los sistemas.

- **Recopilación de evidencias**

  Se debe establecer un procedimiento a seguir en el caso de un incidente de seguridad, para lo cual se debe reunir toda la evidencia involucrada en el caso.

3.2.4.8. Aspectos de seguridad de la información para la gestión de la continuidad del negocio

3.2.4.8.1. Continuidad de seguridad de la información

- **Planificación de la continuidad de la seguridad de la información**

  Se deben definir y documentar todos los procedimientos para respaldar y recuperar la información crítica afectada por incidentes y a su vez garantizar la continuidad del negocio.

  Se debe establecer un manual de procedimientos sobre los tipos de incidentes de seguridad de la información donde se detalle lo siguiente:

GERENCIA DE SEGURIDAD DE LA INFORMACIÓN	DIRECCIÓN GENERAL	GERENCIA DE TECNOLOGÍA
Victoria Camacho Jefe de Seguridad de la Información	Pablo Hidalgo DIRECTOR	Milton Camacho Jefe de TI Curtiembre Quisapincha

- Garantizar que los tiempos de respuesta a incidentes se cumplan.
- Disponer de personal capacitado en el área.
- Realizar respaldos y copias de seguridad a diario, para evitar que un incidente afecte directamente a la información.
- Garantizar redundancia en los equipos de hardware.
- Establecer lineamientos de seguridad de la información en el caso de pérdida de los dispositivos móviles.

- **Implementación de la continuidad de seguridad de la información**
  Se debe garantizar la continuidad del negocio mediante la gestión de respuestas a incidentes, *backup* de sistemas, copias de seguridad y servicios de respaldo para evitar la afectación directa a los activos de información.

- **Verificar, revisar y evaluar la continuidad de seguridad de la información**
  Se deben realizar pruebas continuas del plan de recuperación ante amenazas del tipo desastres naturales o industriales, para garantizar el funcionamiento adecuado de dicho plan, así también la recuperación y continuidad del negocio.

3.2.4.8.2. Redundancias

- **Disponibilidad de las instalaciones de procesamiento de la información**
  Se debe administrar de forma eficiente los equipos que brindan redundancia a servidores y bases de datos; también se debe tener redundancia en el servicio de Internet para evitar fallos en los sistemas que funcionan de forma *online.*

3.2.4.9. Cumplimiento

3.2.4.9.1. Cumplimiento de los requisitos legales y contractuales

- **Derechos de propiedad intelectual**
  Se deben registrar los derechos de autor de las marcas y todos los productos originales de la empresa en el INEN (Servicio Ecuatoriano de Normalización), con el fin de garantizar la propiedad de estos.

GERENCIA DE SEGURIDAD DE LA INFORMACIÓN	DIRECCIÓN GENERAL	GERENCIA DE TECNOLOGÍA
Victoria Camacho Jefe de Seguridad de la Información	Pablo Hidalgo DIRECTOR	Milton Camacho Jefe de TI Curtiembre Quisapincha

4. CONCLUSIONES Y RECOMENDACIONES

4.1. CONCLUSIONES

- Se diseñó el Sistema de Gestión de Seguridad de la Información de la fábrica de cuero y calzado Curtiembre Quisapincha, en función de las normas ISO 27000:2016, ISO27001:2013, ISO27002:2013, ISO 27005:2012 y de la metodología MAGERIT v.3, así como de los requerimientos del Área de Tecnología de Información de la empresa.
- Este proyecto de titulación ha permitido alcanzar los objetivos estratégicos de la empresa ya que permitió levantar información valiosa para el conocimiento de la Alta Dirección, posibilitando que se consolide una estructura segura para el manejo de la información.
- Una vez evaluada la situación actual de la empresa, se determinó que esta requiere de un Sistema de Gestión de Seguridad de la Información, debido a que no cuenta con uno, a pesar de que existen controles que tienen un nivel de madurez inicial (20%) y que por tanto no permiten enfrentar los riesgos de los activos que protege; adicionalmente sus procedimientos no son claros para su uso y no cuenta con controles para combatir incidentes de seguridad de la información.
- En este trabajo de titulación se desarrolló una metodología específica y acorde a los requerimientos de la empresa en función de la metodología MAGERIT v.3 y la norma ISO27001:2013. Esta metodología permitió obtener los resultados de la identificación de activos y su valoración, sus amenazas, el documento de aplicabilidad, niveles de madurez de los controles existentes y seleccionados; permitió también determinar los valores de impacto, riesgos, controles y el tratamiento del riesgo para cada riesgo.
- Durante el desarrollo del diseño del SGSI se generó el levantamiento de información, lo cual permitió identificar que existen 36 activos de información, las brechas de seguridad, amenazas y riesgos; esta información no la conocía el Área de Tecnologías de la Información de la empresa, por lo que ha permitido alertar a la Alta Dirección y al área correspondiente sobre posibles incidentes en su sistema de información.
- La implementación del diseño del Sistema de Gestión de Seguridad de la Información (SGSI), permitirá reducir el nivel de criticidad de los 395 riesgos identificados en los activos de la empresa, con el fin de evitar que las amenazas se materialicen y perjudiquen al giro de negocio de la empresa; y así también permitirá garantizar la Integridad, Confidencialidad y Disponibilidad de la información.

- La telefonía móvil es un activo correspondiente al grupo de redes de comunicaciones que tiene un Riesgo Actual muy crítico; es decir, puede ocasionar altas pérdidas económicas. Su riesgo es alto debido a que actualmente la empresa cuenta con nuevos procesos de ventas en línea y telemercadeo, y no cuenta con controles establecidos para disminuir el riesgo de que existan denegación de servicios, fallo de servicios de comunicaciones, suplantación de identidad, acceso no autorizado, entre otras amenazas consideradas en este análisis.

- Las políticas de seguridad se definieron en función del documento de aplicabilidad, análisis de riesgos y tratamiento de los riesgos. Las mismas se las deben implementar para reducir el nivel de criticidad de los riesgos encontrados en el análisis y evaluación del Riesgo Actual de todos sus activos, a fin de evitar daños y pérdidas económicas para la empresa.

- Es indispensable la capacitación del recurso humano, la misma que debería incluir desde la Alta Dirección, personal interno y externo, clientes y proveedores; también se deberá indicar las amenazas más comunes dentro y fuera de la empresa, explicar el riesgo que genera el recurso humano, cómo evitarlo y la responsabilidad que cada uno conlleva en el sistema de gestión de seguridad de la información.

- Hay activos que son más críticos que otros, por lo tanto, se establecen 64 controles que buscan la continuidad del negocio en todos sus aspectos; uno de estos es mejorar la disponibilidad con redundancia, garantizar la confidencialidad e integridad de datos a través de las políticas de control de acceso y asignar roles y responsabilidades a todos los usuarios del sistema de información de la empresa.

4.2. RECOMENDACIONES

- Una vez elaborado el diseño del SGSI de la empresa Curtiembre Quisapincha, se recomienda a la Alta Dirección evaluar, establecer y aprobar el presupuesto que se requiere para su implementación, pues es un sistema necesario para garantizar y brindar seguridad a la información del núcleo del negocio y a todo el personal involucrado con la empresa como clientes, proveedores y empleados.

- Se recomienda incluir en el diseño del SGSI a los activos y dominios excluidos que son la Seguridad de Recurso Humano, Seguridad Física y Ambiental, Adquisición, Desarrollo y Mantenimiento del Sistema, Relaciones con los Proveedores, así también complementarlo con el análisis de la relación entre los activos de cada proceso.

- La empresa debe implementar el SGSI para mitigar los riesgos a los que están expuestos sus activos, es un proceso a largo plazo y muy costoso, por lo tanto, se recomienda evaluar la capacidad de la empresa y planificar dicha implementación en el lapso de 1 año o 2 años para obtener mejores resultados en función de los resultados actuales.
- Se recomienda iniciar con un plan de capacitación en Sistemas de Gestión de Seguridad de la Información que explique los fundamentos y conceptos básico de seguridades, riesgos y amenazas a los que están expuestos todos los activos incluido el recurso humano.
- Se debe capacitar al personal del Área de Tecnologías de la Información en los temas específicos del SGSI, para que estén en la capacidad de identificar las amenazas que pueden ocasionar daños en los activos, así también concientizar el uso y cuidado de los activos de información. Este proceso se lo puede realizar a través de campañas periódicas de seguridad de la información por parte de los grupos de interés especializados en SGSI.
- Una vez puesto en marcha el SGSI se recomienda al Área de Tecnologías de la Información de la empresa, realizar un monitoreo continuo del sistema de gestión de seguridad de la información, así como generar una planificación periódica para el análisis de los niveles de riesgos actuales y riesgos planificados de los activos.
- Se recomienda también utilizar otras metodologías de análisis y gestión de riesgos, con el fin de establecer comparativas. En este caso se sugiere el uso de la metodología MEHARI debido a que presenta una estructura muy similar a las normas ISO/IEC 27001.

5. BIBLIOGRAFÍA

[1] RiskIQ, «The Evil Internet Minute 2020,» 2020. [En línea]. Available: https://www.riskiq.com/resources/infographic/evil-internet-minute-2020/. [Último acceso: 4 diciembre 2020].

[2] El Mercurio, «Comercio Electrónico una Tendencia Irreversible,» 7 mayo 2020. [En línea]. Available: https://ww2.elmercurio.com.ec/2020/05/07/comercio-electronico-una-tendencia-irreversible/. [Último acceso: 9 julio 2020].

[3] R. Weder, «Search Data Center, Seguridad de la Información,» 29 mayo 2020. [En línea]. Available: https://searchdatacenter.techtarget.com/es/cronica/Seguridad-de-la-informacion-mas-alla-de-la-tecnologia?_ga=2.72673232.2124161670.1598237685-930957924.1598237684. [Último acceso: 10 agosto 2020].

[4] Escuela Europea Excelencia, «Importancia de la Certificación ISO/IEC 27001,» febrero 2019. [En línea]. Available: https://www.escuelaeuropeaexcelencia.com/2019/02/por-que-una-organizacion-deberia-obtener-la-certificacion-en-iso-27001/. [Último acceso: 10 julio 2020].

[5] L. Charlet, «International Organization for Standardization (ISO), Certification & Conformity ISO Survey,» 31 diciembre 2018. [En línea]. Available: https://www.iso.org/the-iso-survey.html. [Último acceso: 10 agosto 2020].

[6] L. Charlet, «ISO Standards Development, ISO Survey of Certifications to Management System Standards,» 11 septiembre 2019. [En línea]. Available: https://isotc.iso.org/livelink/livelink?func=ll&objId=18808772&objAction=browse&viewType=1. [Último acceso: 10 mayo 2020].

[7] F. Mayorga y J. Tigse, «Plan de Gestión de Seguridad Informática basado en la Norma ISO 27001 para el Departamento de Tecnologías de la Información en la Empresa Plasticaucho Industrial S.A.,» 30 enero 2020. [En línea]. Available: https://repositorio.uta.edu.ec/jspui/handle/123456789/30696. [Último acceso: 9 mayo 2020].

[8] B. Institute, «Seguridad de la Información,» 2020. [En línea]. Available: https://bsginstitute.com/bs-campus/blog/seguridad-de-la-informacion-20. [Último acceso: 1 diciembre 2020].

[9] INEN, «TECNOLOGÍAS DE LA INFORMACIÓN –TÉCNICAS DE SEGURIDAD –CÓDIGO DE PRÁCTICA PARA LOS CONTROLES DE SEGURIDAD DE LA INFORMACIÓN (ISO/IEC 27002:2013+Cor.1:2014+Cor.2: 2015, IDT)». Ecuador Patente NTE INEN-ISO/IEC27002, abril 2017.

[10] Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica del Gobierno de España, «MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I - Método,» octubre 2012. [En línea]. Available: https://administracionelectronica.gob.es/pae_Home/dam/jcr:fb373672-f804-4d05-8567-2d44b3020387/2012_Magerit_v3_libro1_metodo_es_NIPO_630-12-171-8.pdf. [Último acceso: 10 marzo 2021].

[11] Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica del Gobierno de España, «MAGERIT - versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información: Libro II - Catálogo de Elementos,» octubre 2012. [En línea]. Available: https://administracionelectronica.gob.es/pae_Home/dam/jcr:5fbe15c3-c797-46a6-acd8-51311f4c2d29/2012_Magerit_v3_libro2_catalogo-de-elementos_es_NIPO_630-12-171-8.pdf. [Último acceso: 16 febrero 2021].

[12] INEN, «TECNOLOGÍASDE LA INFORMACIÓN —TÉCNICAS DE SEGURIDAD — SISTEMASDE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN — DESCRIPCIÓN GENERAL Y VOCABULARIO (ISO/IEC27000:2016,IDT)». Ecuador Patente NTE INEN-ISO/IEC 27000, noviembre 2016.

[13] Grupo Respuesta a Incidentes de Seguridad de la Escuela Politécnica Nacional-CSIRTEPN, «“Evento inesperado que compromete la operación de un sistema y su información, amenazando la confidencialidad, integridad o disponibilidad”,» 2020. [En línea]. Available: https://www.csirt-epn.edu.ec/2-uncategorised/35-lista-de-incidentes. [Último acceso: 6 diciembre 2020].

[14] INEN, «TECNOLOGÍAS DE LA INFORMACIÓN —TÉCNICAS DE SEGURIDAD — SISTEMAS DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN –

REQUISITOS(ISO/IEC 27001:2013+Cor.1:2014+ Cor. 2:2015, IDT)». Ecuador Patente NTE INEN-ISO/IEC 27001, enero 2017.

[15] K. Bird y E. Gasiosowski-Denis, «Secretos Ciberneticos,» 2019. [En línea]. Available: https://www.iso.org/files/live/sites/isoorg/files/news/magazine/ISOfocus%20(2013-NOW)/sp/ISOfocus_132_sp.pdf. [Último acceso: 7 julio 2020].

[16] A. Mejía, «Norma ISO/IEC 27001:2013- Estructura». Quito - Ecuador 2013.

[17] INEN, «TECNOLOGÍA DE LA INFORMACIÓN-TÉCNICAS DE SEGURIDAD-GESTIÓN DEL RIESGO EN LA SEGURIDAD DE LA INFORMACIÓN NTE INEN-ISO/IEC 27005:2012-». Ecuador Patente NTE INEN-ISO/IEC 27005:2012, mayo 2012.

[18] Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica del Gobierno de España, «MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro III - Guía de Técnicas,» octubre 2012. [En línea]. Available: https://administracionelectronica.gob.es/pae_Home/dam/jcr:130c633a-ee11-4e17-9cec-1082ceeac38c/2012_Magerit_v3_libro3_guia-de-tecnicas_es_NIPO_630-12-171-8.pdf. [Último acceso: 10 febrero 2020].

[19] welivesecurity by ESET, «¿Qué es una Declaración de Aplicabilidad (SoA) y para qué sirve?,» 1 abril 2015. [En línea]. Available: https://www.welivesecurity.com/la-es/2015/04/01/que-es-declaracion-de-aplicabilidad-soa/#:~:text=SoA%20se%20trata%20de%20un,de%20esta%20norma%20de%20seguridad).. [Último acceso: 15 mayo 2021].

[20] CURTIEMBRE QUISAPINCHA, «Quisapincha Curtiembre: Quienes Somos,» enero 2020. [En línea]. Available: https://www.curtiembrequisapincha.com/quienes-somos/. [Último acceso: 25 octubre 2020].

[21] CURTIEMBRE QUISAPINCHA, Estructura Organizacional de la Empresa, Ambato, 2021.

[22] CURTIEMBRE QUISAPINCHA, Infraestructura Tecnologica de la Empresa, Ambato, 2021.

[23] «Intercompras, Servidor HP-DL360P-Gen8,» [En línea]. Available: https://intercompras.com/p/servidor-hp-dl360p-gen-e5-2630v2-6c-1p-16gb-1gb-sff-74728. [Último acceso: 10 febrero 2021].

[24] «PROXMOX,» [En línea]. Available: https://www.proxmox.com/en/proxmox-ve. [Último acceso: 5 febrero 2021].

[25] BeServices, «Servidor virtual: Qué es y principales características,» 21 agosto 2019. [En línea]. Available: https://www.beservices.es/que-un-servidor-virtual-caracteristicas-n-5392-es. [Último acceso: 18 febrero 2021].

[26] Redes Zone, «Virtualiza Sistemas Operativos con Proxmox Virtual Environment,» [En línea]. Available: https://www.redeszone.net/2015/01/03/virtualiza-sistemas-operativos-con-proxmox-virtual-environment/. [Último acceso: 10 febrero 2021].

[27] S. Cheng, «Proxmox High Availability,» Packt Publishing Ltd, 2014. [En línea]. Available: https://books.google.com.ec/books?id=PtskBQAAQBAJ&pg=PT32&redir_esc=y#v=onepage&q&f=false. [Último acceso: 11 febrero 2021].

[28] K. John, «Computing For Geeks-¿Cuáles son las nuevas funciones de CentOS 8?,» 15 octubre 2019. [En línea]. Available: https://computingforgeeks.com/centos-released-centos-8-new-features/. [Último acceso: 18 febrero 2021].

[29] APEN, «APEN.ES: ¿Que es un Switch?,» [En línea]. Available: https://apen.es/glosario-de-informatica/switch/#:~:text=El%20switch%20es%20un%20dispositivo,especificaciones%20t%C3%A9cnicas%20del%20est%C3%A1ndar%20Ethernet.&text=Switches%3B%20se%20encargan%20de%20la,dentro%20de%20una%20misma%20red. [Último acceso: 8 marzo 2020].

[30] TP-LINK, «Switches no Gestionables TL-SG1024D,» [En línea]. Available: https://www.tp-link.com/es/business-networking/unmanaged-switch/tl-sg1024d/. [Último acceso: 1 marzo 2021].

[31] Syscom, «Syscom: DVR/NVR,» [En línea]. Available: https://www.syscom.mx/producto/DS-7216HQHI-F2-HIKVISION-85253.html. [Último acceso: 28 febrero 2021].

[32] BBVA, «Token Digital,» [En línea]. Available: https://www.bbva.pe/personas/servicios-digitales/token-digital.html. [Último acceso: 2 febrero 2021].

[33] NEXTU, «Tipos de Servidores,» [En línea]. Available: https://www.nextu.com/blog/tipos-de-servidores/. [Último acceso: 18 febrero 2021].

[34] Oracle, «ORACLE,» [En línea]. Available: https://www.oracle.com/es/database/technologies/appdev/xe.html. [Último acceso: 22 febrero 2021].

[35] MySQL, ««MySQL-Manual de referencia de MySQL 8.0,» [En línea]. Available: https://dev.mysql.com/doc/refman/8.0/en/features.html. [Último acceso: 21 febrero 2021].

[36] PostgreSQL, «PostgreSQL- PostgreSQL 13.2, 12.6, 11.11, 10.16, 9.6.21 y 9.5.25,» febrero 2020. [En línea]. Available: https://www.postgresql.org/about/. [Último acceso: 25 febrero 2021].

[37] OwnCloud, «OwnCloud,» [En línea]. Available: https://owncloud.com/es/. [Último acceso: 22 febrero 2021].

[38] E. Bonet, «Servidores de ficheros mediante FTP y TFTP,» [En línea]. Available: http://informatica.uv.es/it3guia/AGR/apuntes/teoria/documentos/FTP.pdf. [Último acceso: 15 enero 2021].

[39] ACENS, «Servidor web Nginx, una clara alternativa a Apache,» septiembre 2013. [En línea]. Available: https://www.acens.com/wp-content/images/2013/09/servidor-web-nginx-white-paper-acens.pdf. [Último acceso: 15 enero 2021].

[40] I. Calvopiña, «SACI COMUNIDAD DE USUARIOS,» [En línea]. Available: https://www.sacijava.com/. [Último acceso: 15 marzo 2021].

[41] W. Stallings, Cryptography and Network Security, sixth ed., Pearson, 2014.

[42] D. Comer y D. Stevens, Internetworking with TCP/IP, vol. III, Prentice Hall, 1993.

[43] LCTD CORP, «LCDT CORP: Central Telefónica Panasonic,» [En línea]. Available: https://lcdtcorp.com/products/central-telefonica-panasonic-kx-tes824-pbx-analoga-con-3-lineas-y-8-extensiones. [Último acceso: 5 marzo 2021].

ANEXOS

ANEXO A. ENTREVISTA

ANEXO B. COSTO DEL ACTIVO

ANEXO C. COSTO POR DIMENSIONES

ANEXO D. VALOR DEL ACTIVO

ANEXO E. IDENTIFICACIÓN Y VALORACIÓN DE AMENAZAS

ANEXO F. VALORACIÓN DEL IMPACTO POTENCIAL

ANEXO G. VALORACIÓN DEL RIESGO POTENCIAL

ANEXO H. ACEPTACIÓN Y TRATAMIENTO DEL RIESGO

ANEXO I. ANÁLISIS DEL RIESGO PLANIFICADO

A. ANEXO A: ENTREVISTA

ENTREVISTA DIRIGIDA AL JEFE DEL ÁREA DE TECNOLOGÍAS DE LA INFORMACIÓN DE LA EMPRESA CURTIEMBRE QUISAPINCHA

TEMA: IDENTIFICACIÓN DE BRECHAS, INCIDENTES Y RIESGOS DE SEGURIDAD EXISTENTES EN LA SEGURIDAD DE LA INFORMACIÓN DE LA EMPRESA.

ENTREVISTA DIRIGIDA AL JEFE DEL ÁREA DE TECNOLOGÍAS DE LA INFORMACIÓN DE LA EMPRESA CURTIEMBRE QUISAPINCHA

TEMA: IDENTIFICACIÓN DE BRECHAS, INCIDENTES Y RIESGOS DE SEGURIDAD EXISTENTES EN LA SEGURIDAD DE LA INFORMACIÓN DE LA EMPRESA.

CUESTIONARIO:

1. **¿Ha tenido algún tipo de incidente de seguridad en la información de la empresa?**

   Si, si ha habido incidentes de seguridad en la empresa que nos han perjudicado de manera directa. Uno de los incidentes más importantes fue la filtración de datos de la cartera de clientes potenciales del área de ventas.

2. **¿Considera que existen brechas de seguridad de la información?**

   Si, si existen brechas de seguridad de la información, debido a que no se tiene establecido un proceso de control de acceso en todos los computadores.

3. **¿Se realizan campañas de concientización al usuario en temas de seguridad de la información?**

   No, la empresa no realiza campañas de concientización referente a seguridad de la información, pese a los incidentes ocurridos.

4. **Los sistemas internos de la empresa, ¿tienen definidos roles y perfiles para los usuarios?**

   Si, el sistema contable si tiene roles definidos para cada usuario según un perfil especifico, pero no se tienen definidos perfiles de acceso a los sistemas operativos de los computadores.

5. **¿Qué tipo de información considera que es confidencial en la empresa?**

   La información confidencial de la empresa se considera a todo tipo de información física o digital referente a clientes, proveedores y productos de la empresa.

6. **¿Cuáles son los servicios externos más críticos que la empresa utiliza dentro del giro del negocio?**

El servicio de Internet es el principal servicio externo que la empresa consume diariamente, debido a que los servidores de bases de datos están alojados en la nube y se requiere de conectividad todo el tiempo para hacer uso de dichas bases.

7. **¿Existen políticas de seguridad de la información?**

   No, no existen políticas de seguridad de la información definidas.

8. **¿Existen procedimientos documentados relacionados a la seguridad de la información?**

   No, no existen procedimientos documentados relacionados con la seguridad de la información.

9. **¿Cuáles son los mayores riesgos en la seguridad de la información que existen en la empresa?**

   El mayor riesgo que existe es la perdida de las bases de datos de la parte administrativa de la empresa.

10. **¿Considera existe fugas de información confidencial de la empresa?**

    Si, si ha existido fugas de información dentro de la empresa, la fuga de información referente a formulaciones químicas del cuero del área de producción de cuero fue una de las más graves debido a que es información confidencial.

B. ANEXO B: COSTO DEL ACTIVO

- **[INFO] INFORMACIÓN**

Tabla B.1. Costo del Activo: Información

COSTO DEL ACTIVO: [INFO] INFORMACIÓN						
CÓDIGO	ACTIVO	CO	DE	COSTO DEL ACTIVO		
				EX	EN	DESCRIPCIÓN
[INFO_PER]	Base de datos de clientes y proveedores	4	5	9	5	Crítico
[INFO_PUB]	Documentación y permisos de funcionamiento	5	5	10	5	Crítico
[INFO_VR]	Registros confidenciales de la organización	3	5	8	4	Muy importante

- **[D] DATOS E INFORMACIÓN COMPLEMENTARIA**

Tabla B.2. Costo del Activo: Datos e Información Complementaria

COSTO DEL ACTIVO: [D] DATOS E INFORMACIÓN COMPLEMENTARIA						
CÓDIGO	ACTIVO	CO	DE	COSTO DEL ACTIVO		
				EX	EN	DESCRIPCIÓN
[D_LG]	Logs de SACI	1	5	6	3	Importante
[D_BCK]	Copias de seguridad *OwnCloud*	1	5	6	3	Importante

- **[K] CLAVES CRIPTOGRÁFICAS**

Tabla B.3. Costo del Activo: Claves Criptográficas

COSTO DEL ACTIVO: [K] CLAVES CRIPTOGRÁFICAS						
CÓDIGO	ACTIVO	CO	DE	COSTO DEL ACTIVO		
				EX	EN	DESCRIPCIÓN
[K_PB]	SSL	1	4	5	3	Importante
[K_SIGN]	*Token* Digital	1	4	5	3	Importante

- **[S] SERVICIOS**

Tabla B.4. Costo del Activo: Servicios

COSTO DEL ACTIVO: [S] SERVICIOS						
CÓDIGO	ACTIVO	CO	DE	COSTO DEL ACTIVO		
				EX	EN	DESCRIPCIÓN
[S_INT]	Servicio del sistema contable	4	4	8	4	Muy importante
[S_WWW]	Sitio web	3	3	6	3	Importante

- **[SW] SOFTWARE- APLICACIONES INFORMÁTICAS**

Tabla B.5. Costo del Activo: Software - Aplicaciones Informáticas

COSTO DEL ACTIVO: [SW] SOFTWARE- APLICACIONES INFORMÁTICAS						
CÓDIGO	ACTIVO	CO	DE	COSTO DEL ACTIVO		
				EX	EN	DESCRIPCIÓN
[SW_HP]	Proxmox	2	5	7	4	Muy importante
[SW_APP4]	Servidor Digital Ocean	3	4	7	4	Muy importante
[SW_BD1]	Servidor de Base de Datos Oracle XE 18c	3	5	8	4	Muy importante
[SW_APP2]	Servidor FTP	2	4	6	3	Importante
[SW_BD2]	Servidor de Base de Datos MySQL 8.0	3	3	6	3	Importante
[SW_AV]	A*vast Free Antivirus*	1	3	4	2	Poco Importante
[SW_APP1]	Servidor de OwnCloud	2	3	5	3	Importante
[SW_APP3]	Servidor DNS	2	4	6	3	Importante
[SW_BD3]	Servidor de Base de Datos Postgresql 13	3	3	6	3	Importante
[SW_WWW]	Servidor Web NGINX	1	3	4	2	Poco Importante
[SW_ALM]	Google Drive	2	2	4	2	Poco Importante
[SW_OFF]	Microsoft Office Professional 2019	1	2	3	2	Poco Importante
[SW_OS]	Windows/Linux	1	3	4	2	Poco Importante

- **[HW] HARDWARE- EQUIPOS INFORMÁTICOS**

Tabla B.6. Costo del Activo: Hardware – Equipos Informáticos

COSTO DEL ACTIVO: [HW] HARDWARE- EQUIPOS INFORMÁTICOS						
CÓDIGO	ACTIVO	CO	DE	COSTO DEL ACTIVO		
				EX	EN	DESCRIPCIÓN
[SW_HT]	Servidor físico HP Proliant DL 360P	5	5	10	5	Crítico
[SW_SW]	*Switch* TP-LINK	4	5	9	5	Crítico
[SW_MV2]	Teléfonos móviles	3	5	8	4	Muy importante
[SW_PC]	Computadoras de escritorio	4	4	8	4	Muy importante
[SW_MV1]	Computadoras Portátiles	4	4	8	4	Muy importante
[SW_WAP]	Punto de Acceso	3	3	6	3	Importante
[SW_PT]	Impresoras	3	3	6	3	Importante

- **[COM] REDES DE COMUNICACIONES**

Tabla B.7. Costo del Activo: Redes de Comunicaciones

COSTO DEL ACTIVO: [COM] REDES DE COMUNICACIONES						
CÓDIGO	ACTIVO	CO	DE	COSTO DEL ACTIVO		
				EX	EN	DESCRIPCIÓN
[COM_INT]	Internet Fibra Óptica	5	5	10	5	Crítico
[COM_WF]	Red Inalámbrica	3	5	8	4	Muy importante
[COM_LAN]	Red Local	4	5	9	5	Crítico
[COM_MB]	Telefonía Móvil	3	4	7	4	Muy importante

- **[AUX] EQUIPO AUXILIAR**

Tabla B.8. Costo del Activo: Equipo Auxiliar

COSTO DEL ACTIVO: [AUX] EQUIPO AUXILIAR						
CÓDIGO	ACTIVO	CO	DE	COSTO DEL ACTIVO		
				EX	EN	DESCRIPCIÓN
[AUX_CB]	Cableado Estructurado	5	4	9	5	Crítico
[AUX_UPS]	Sistema de alimentación Interrumpida	3	5	8	4	Muy importante
[AUX_VIDEO]	Sistema de Video vigilancia	5	3	8	4	Muy importante

C. ANEXO C: COSTO POR DIMENSIONES

- **INFORMACIÓN**

Tabla C.1. Costo por dimensiones del activo: Información

COSTO POR DIMENSIONES DEL ACTIVO: [INFO] INFORMACIÓN																										
CÓDIGO	ACTIVO	[i] INTEGRIDAD						[c] CONFIDENCIALIDAD							[d] DISPONIBILIDAD									COSTO DIMENSIONES		
		[si]	[cei]	[adm]	[lg]	VT	VP	[si]	[cei]	[adm]	[lg]	[rto]	VT	VP	[si]	[cei]	[da]	[adm]	[lg]	[rto]	VT	VP	EX	EN	NIVEL
[INFO_PER]	Base de datos de clientes y proveedores	5	5	4	5	19	5	5	5	5	5	5	25	5	5	5	5	4	5	5	29	5	15	5	CRITICO
[INFO_PUB]	Documentación y permisos de funcionamiento	3	5	5	5	18	5	2	5	2	3	3	15	3	5	5	5	5	5	4	29	5	13	5	CRITICO
[INFO_VR]	Registros confidenciales de la organización	5	5	4	5	19	5	5	5	4	5	4	23	5	4	5	4	4	5	5	27	5	15	5	CRITICO

- **DATOS E INFORMACIÓN COMPLEMENTARIA**

Tabla C.2. Costo por dimensiones del activo: Datos e Información Complementaria

COSTO POR DIMENSIONES DEL ACTIVO: [D] DATOS E INFORMACIÓN COMPLEMENTARIA																										
CÓDIGO	ACTIVO	[i] INTEGRIDAD						[c] CONFIDENCIALIDAD							[d] DISPONIBILIDAD									COSTO DIMENSIONES		
		[si]	[cei]	[adm]	[lg]	VT	VP	[si]	[cei]	[adm]	[lg]	[rto]	VT	VP	[si]	[cei]	[da]	[adm]	[lg]	[rto]	VT	VP	EX	EN	NIVEL
[D_LG]	Logs de SACI	5	2	1	2	10	3	3	5	2	3	2	15	3	2	5	3	2	3	3	18	3	9	3	IMPORTANTE
[D_BCK]	Copias de seguridad OwnCloud	5	3	1	2	11	3	5	3	2	3	3	16	4	1	3	3	2	3	3	15	3	10	4	MUY IMPORTANTE

- **CLAVES CRIPTOGRÁFICAS**

Tabla C.3. Costo por dimensiones del activo: Claves Criptográficas

COSTO POR DIMENSIONES DEL ACTIVO: [K] CLAVES CRIPTOGRÁFICAS																										
CÓDIGO	ACTIVO	[i] INTEGRIDAD						[c] CONFIDENCIALIDAD							[d] DISPONIBILIDAD									COSTO DIMENSIONES		
		[si]	[cei]	[adm]	[lg]	VT	VP	[si]	[cei]	[adm]	[lg]	[rto]	VT	VP	[si]	[cei]	[da]	[adm]	[lg]	[rto]	VT	VP	EX	EN	NIVEL
[K_PB]	SSL	5	5	2	5	17	5	5	5	3	5	5	23	5	5	5	3	2	5	5	25	5	15	5	CRITICO
[K_SIGN]	Token Digital	3	4	2	2	11	3	3	4	3	4	1	15	3	2	4	2	2	3	2	15	3	9	3	IMPORTANTE

- **SERVICIOS**

Tabla C.4. Costo por dimensiones del activo: Servicios

COSTO POR DIMENSIONES DEL ACTIVO: [S] SERVICIOS																										
CÓDIGO	ACTIVO	[i] INTEGRIDAD						[c] CONFIDENCIALIDAD							[d] DISPONIBILIDAD									COSTO DIMENSIONES		
		[si]	[cei]	[adm]	[lg]	VT	VP	[si]	[cei]	[adm]	[lg]	[rto]	VT	VP	[si]	[cei]	[da]	[adm]	[lg]	[rto]	VT	VP	EX	EN	NIVEL
[S_INT]	Servicio del sistema contable	5	5	4	4	18	5	5	5	4	5	5	24	5	4	5	4	4	5	5	27	5	15	5	CRITICO
[S_WWW]	Sitio web	3	3	3	5	14	4	2	5	3	4	4	18	4	2	5	3	3	5	5	23	4	12	4	MUY IMPORTANTE

- **SOFTWARE – APLICACIONES INFORMÁTICAS**

Tabla C.5. Costo por dimensiones del activo: Software – Aplicaciones Informáticas

COSTO POR DIMENSIONES DEL ACTIVO: [SW] SOFTWARE- APLICACIONES INFORMÁTICAS																								
CÓDIGO	ACTIVO	[i] INTEGRIDAD						[c] CONFIDENCIALIDAD							[d] DISPONIBILIDAD								COSTO DIMENSIONES		
		[si]	[cei]	[adm]	[lg]	VT	VP	[si]	[cei]	[adm]	[lg]	[rto]	VT	VP	[si]	[cei]	[da]	[adm]	[lg]	[rto]	VT	VP	EX	EN	NIVEL
[SW_HP]	Proxmox	5	5	3	3	16	4	5	5	4	4	5	23	5	5	4	5	5	5	5	29	5	14	5	CRITICO
[SW_APP4]	Servidor Digital Ocean	2	3	2	2	9	4	5	3	3	3	5	19	4	2	3	3	2	5	5	20	4	12	4	MUY IMPORTANTE
[SW_BD1]	Servidor de Base de Datos Oracle XE 18c	5	5	4	5	19	5	5	5	4	5	5	24	5	4	5	5	5	5	5	29	5	15	5	CRITICO
[SW_APP2]	Servidor FTP	5	5	3	4	17	5	5	5	3	4	4	21	5	3	4	5	3	2	5	22	4	14	5	CRITICO
[SW_BD2]	Servidor de Base de Datos MySQL 8.0	4	4	3	3	14	4	5	4	3	4	4	20	4	3	4	5	3	3	5	23	4	12	4	MUY IMPORTANTE
[SW_AV]	Avast Free Antivirus	5	2	2	1	10	3	5	2	2	1	2	12	5	5	1	3	2	1	4	16	3	11	4	MUY IMPORTANTE
[SW_APP1]	Servidor de OwnCloud	5	3	2	2	12	3	5	3	2	1	2	13	3	2	1	3	2	2	3	13	3	9	3	IMPORTANTE
[SW_APP3]	Servidor DNS	3	4	4	4	15	4	3	4	4	4	4	19	4	4	4	4	4	4	5	25	5	13	5	CRITICO
[SW_BD3]	Servidor de Base de Datos Postgresql 13	3	4	2	3	12	3	3	4	3	4	3	17	4	2	4	3	2	3	3	17	3	10	4	MUY IMPORTANTE
[SW_WWW]	Servidor Web NGINX	2	2	2	3	9	3	3	2	2	2	2	11	3	2	2	3	1	4	3	15	3	9	3	IMPORTANTE
[SW_ALM]	Google Drive	2	1	1	2	6	2	4	1	1	1	1	8	2	1	1	3	1	2	2	10	2	6	2	POCO IMPORTANTE
[SW_OFF]	Microsoft Office Professional 2019	1	2	1	1	5	2	1	2	1	1	1	6	2	1	1	2	1	1	4	10	2	6	2	POCO IMPORTANTE
[SW_OS]	Windows/Linux	3	2	1	2	8	2	2	2	1	1	1	7	2	1	1	5	1	1	5	14	3	7	3	IMPORTANTE

- **HARDWARE – EQUIPOS INFORMÁTICOS**

Tabla C.6. Costo por dimensiones del activo: Hardware - Equipos Informáticos

COSTO POR DIMENSIONES DEL ACTIVO: [HW] HARWARE- EQUIPOS INFORMÁTICOS																								
CÓDIGO	**ACTIVO**	**[i] INTEGRIDAD**						**[c] CONFIDENCIALIDAD**							**[d] DISPONIBILIDAD**								**COSTO DIMENSIONES**		
		[si]	[cei]	[adm]	[lg]	**VT**	**VP**	[si]	[cei]	[adm]	[lg]	[rto]	**VT**	**VP**	[si]	[cei]	[da]	[adm]	[lg]	[rto]	**VT**	**VP**	**EX**	**EN**	**NIVEL**
[SW_HT]	Servidor físico HP Proliant DL 360P	5	4	4	4	17	5	5	5	4	5	5	24	5	5	5	5	5	5	5	30	5	15	5	CRITICO
[SW_SW]	Switch TP-LINK	4	4	3	2	13	4	2	3	3	3	4	15	3	2	3	5	3	4	5	22	4	11	4	MUY IMPORTANTE
[SW_MV2]	Teléfonos móviles	5	5	3	5	18	5	5	5	3	5	5	23	5	3	5	5	5	5	5	28	5	15	5	CRITICO
[SW_PC]	Computadoras de escritorio	5	4	2	4	15	4	5	4	2	3	4	18	4	2	3	3	4	4	4	20	4	12	4	MUY IMPORTANTE
[SW_MV1]	Computadoras Portátiles	5	4	2	4	15	4	5	4	2	3	4	18	4	2	3	3	4	4	4	20	4	12	4	MUY IMPORTANTE
[SW_WAP]	Punto de Acceso	5	2	1	3	11	3	5	2	1	1	3	12	3	2	1	3	1	4	3	14	3	9	3	IMPORTANTE
[SW_PT]	Impresoras	1	1	1	1	4	1	1	2	1	1	1	6	2	1	1	2	2	1	3	10	2	5	2	POCO IMPORTANTE

- **REDES DE COMUNICACIONES**

Tabla C.7. Costo por dimensiones del activo: Redes de Comunicaciones

COSTO POR DIMENSIONES DEL ACTIVO: [COM] REDES DE COMUNICACIONES																									
CÓDIGO	**ACTIVO**	**[i] INTEGRIDAD**						**[c] CONFIDENCIALIDAD**							**[d] DISPONIBILIDAD**									**COSTO DIMENSIONES**		
		[si]	[cei]	[adm]	[lg]	**VT**	**VP**	[si]	[cei]	[adm]	[lg]	[rto]	**VT**	**VP**	[si]	[cei]	[da]	[adm]	[lg]	[rto]	**VT**	**VP**	**EX**	**EN**	**NIVEL**
[COM_INT]	Internet Fibra Óptica	5	4	4	5	18	5	5	4	4	3	5	21	5	1	3	5	5	5	5	24	4	14	5	CRITICO
[COM_WF]	Red Inalámbrica	5	3	2	5	15	4	5	3	2	4	3	17	4	2	4	3	4	5	4	22	4	12	4	MUY IMPORTANTE
[COM_LAN]	Red Local	5	3	4	4	16	4	5	3	4	5	5	22	5	4	5	5	4	5	5	28	5	14	5	CRITICO
[COM_MB]	Telefonía Móvil	5	5	3	5	18	5	5	5	3	5	5	23	5	5	5	3	3	5	5	26	5	15	5	CRITICO

- **EQUIPO AUXILIAR**

Tabla C.8. Costo por dimensiones del activo: Equipo Auxiliar

COSTO POR DIMENSIONES DEL ACTIVO: [AUX] EQUIPO AUXILIAR																									
CÓDIGO	**ACTIVO**	**[i] INTEGRIDAD**						**[c] CONFIDENCIALIDAD**							**[d] DISPONIBILIDAD**									**COSTO DIMENSIONES**		
		[si]	[cei]	[adm]	[lg]	**VT**	**VP**	[si]	[cei]	[adm]	[lg]	[rto]	**VT**	**VP**	[si]	[cei]	[da]	[adm]	[lg]	[rto]	**VT**	**VP**	**EX**	**EN**	NIVEL
[AUX_CB]	Cableado Estructurado	1	2	3	3	9	3	4	2	2	2	5	15	3	2	2	5	4	5	5	23	4	10	4	MUY IMPORTANTE
[AUX_UPS]	Sistema de alimentación Interrumpida	1	2	1	2	6	2	1	2	1	1	1	6	2	1	1	4	1	2	1	10	2	6	2	POCO IMPORTANTE
[AUX_VIDEO]	Sistema de Video vigilancia	5	4	2	2	13	3	5	3	1	5	3	17	4	5	5	2	1	2	4	19	4	11	4	MUY IMPORTANTE

D. ANEXO D: VALOR DEL ACTIVO

- **[INFO] INFORMACIÓN**

Tabla D.1. Valor del Activo: Información

VALOR DEL ACTIVO: [INFO] INFORMACIÓN						
CÓDIGO	**ACTIVO**	**COSTO DEL ACTIVO**	**COSTO POR DIMENSIONES**	**VALOR ACTIVO**		
				EX	**EN**	**DESCRIPCIÓN**
[INFO_VR]	Registros confidenciales de la organización	5	5	10	5	MUY ALTO
[INFO_PER]	Base de datos de clientes y proveedores	5	5	10	5	MUY ALTO
[INFO_PUB]	Documentación y permisos de funcionamiento	4	5	9	5	MUY ALTO

- **[D] DATOS E INFORMACIÓN COMPLEMENTARIA**

Tabla D.2. Valor del Activo: Datos e Información Complementaria

VALOR DEL ACTIVO: [D] DATOS E INFORMACIÓN COMPLEMENTARIA						
CÓDIGO	**ACTIVO**	**COSTO DEL ACTIVO**	**COSTO POR DIMENSIONES**	**VALOR ACTIVO**		
				EX	**EN**	**DESCRIPCIÓN**
[D_BCK]	Copias de seguridad *OwnCloud*	3	4	7	4	ALTO
[D_LG]	Logs de SACI	3	3	6	3	MODERADO

- **[K] CLAVES CRIPTOGRÁFICAS**

Tabla D.3. Valor del Activo: Claves Criptográficas

VALOR DEL ACTIVO: [K] CLAVES CRIPTOGRÁFICAS						
CÓDIGO	**ACTIVO**	**COSTO DEL ACTIVO**	**COSTO POR DIMENSIONES**	**VALOR ACTIVO**		
				EX	**EN**	**DESCRIPCIÓN**
[K_PB]	SSL	3	5	8	4	ALTO
[K_SIGN]	*Token* Digital	3	3	6	3	MODERADO

- **[S] SERVICIOS**

Tabla D.4. Valor del Activo: Servicios

VALOR DEL ACTIVO: [S] SERVICIOS						
CÓDIGO	**ACTIVO**	**COSTO DEL ACTIVO**	**COSTO POR DIMENSIONES**	**VALOR ACTIVO**		
				EX	**EN**	**DESCRIPCIÓN**
[S_INT]	Servicio del sistema contable	4	5	9	5	MUY ALTO
[S_WWW]	Sitio web	3	4	7	4	ALTO

- **[SW] SOFTWARE- APLICACIONES INFORMÁTICAS**

Tabla D.5. Valor del Activo: Software – Aplicaciones Informáticas

VALOR DEL ACTIVO: [SW] SOFTWARE- APLICACIONES INFORMÁTICAS						
CÓDIGO	ACTIVO	COSTO DEL ACTIVO	COSTO POR DIMENSIONES	VALOR ACTIVO		
				EX	EN	DESCRIPCIÓN
[SW_HP]	Proxmox	4	5	9	5	MUY ALTO
[SW_BD1]	Servidor de Base de Datos Oracle XE 18c	4	5	9	5	MUY ALTO
[SW_APP4]	Servidor Digital Ocean	4	4	8	4	ALTO
[SW_APP2]	Servidor FTP	3	5	8	4	ALTO
[SW_BD2]	Servidor de Base de Datos MySQL 8.0	3	4	7	4	ALTO
[SW_APP3]	Servidor DNS	3	5	8	4	ALTO
[SW_BD3]	Servidor de Base de Datos Postgresql 13	3	4	7	4	ALTO
[SW_AV]	Avast Free Antivirus	2	4	6	3	MODERADO
[SW_APP1]	Servidor de OwnCloud	3	3	6	3	MODERADO
[SW_WWW]	Servidor Web NGINX	2	3	5	3	MODERADO
[SW_OS]	Windows/Linux	2	3	5	3	MODERADO
[SW_ALM]	Google Drive	2	2	4	2	BAJO
[SW_OFF]	Microsoft Office Professional 2019	2	2	4	2	BAJO

- **[HW] HARDWARE- EQUIPOS INFORMÁTICOS**

Tabla D.6. Valor del Activo: Hardware – Equipos Informáticos

VALOR DEL ACTIVO: [HW] HARDWARE- EQUIPOS INFORMÁTICOS						
CÓDIGO	ACTIVO	COSTO DEL ACTIVO	COSTO POR DIMENSIONES	VALOR ACTIVO		
				EX	EN	DESCRIPCIÓN
[SW_HT]	Servidor físico HP Proliant DL 360P	5	5	10	5	MUY ALTO
[SW_SW]	Switch TP-LINK	5	4	9	5	MUY ALTO
[SW_MV2]	Teléfonos móviles	4	5	9	5	MUY ALTO
[SW_PC]	Computadoras de escritorio	4	4	8	4	ALTO
[SW_MV1]	Computadoras Portátiles	4	4	8	4	ALTO
[SW_WAP]	Punto de Acceso	3	3	6	3	MODERADO
[SW_PT]	Impresoras	3	2	5	3	MODERADO

- **[COM] REDES DE COMUNICACIONES**

Tabla D.7. Valor del Activo: Redes de Comunicaciones

VALOR DEL ACTIVO: [COM] REDES DE COMUNICACIONES						
CÓDIGO	ACTIVO	COSTO DEL ACTIVO	COSTO POR DIMENSIONES	VALOR ACTIVO		
				EX	EN	DESCRIPCION
[COM_INT]	Internet Fibra Óptica	5	5	10	5	MUY ALTO
[COM_LAN]	Red Local	5	5	10	5	MUY ALTO
[COM_MB]	Telefonía Móvil	4	5	9	5	MUY ALTO
[COM_WF]	Red Inalámbrica	4	4	8	4	ALTO

- **[AUX] EQUIPO AUXILIAR**

Tabla D.8. Valor del Activo: Equipo Auxiliar

VALOR DEL ACTIVO: [AUX] EQUIPO AUXILIAR						
CÓDIGO	ACTIVO	COSTO DEL ACTIVO	COSTO POR DIMENSIONES	VALOR ACTIVO		
				EX	EN	DESCRIPCION
[AUX_CB]	Cableado Estructurado	5	4	9	5	MUY ALTO
[AUX_VIDEO]	Sistema de Video vigilancia	4	4	8	4	ALTO
[AUX_UPS]	Sistema de alimentación Interrumpida	4	2	6	3	MODERADO

E. ANEXO E: IDENTIFICACIÓN Y VALORACIÓN DE AMENAZAS

- **INFORMACIÓN: [INFO_VR] Registros confidenciales de la organización**

Tabla E.1. Matriz de identificación y valoración de amenazas [INFO_VR]

[INFO] INFORMACIÓN									
[INFO_VR]	**Registros confidenciales de la organización**								
TIPO DE AMENAZAS	**AMENAZAS**	**Dv: DEGRADACIÓN DE VALOR POR DIMENSIONES**						**PROBABILIDAD DE OCURRENCIA**	
		Dv-i	**Dv-c**	**Dv-d**	**Dt-ex**	**DT**	**NIVEL**	**Po**	**NIVEL**
5.3. [E] Errores y fallos no intencionados	5.3.1. [E.1] Errores de los usuarios	5	5	5	15	5	MUY ALTO	5	MUY FRECUENTE
	5.3.2. [E.2] Errores del administrador	5	5	5	15	5	MUY ALTO	5	MUY FRECUENTE
	5.3.10. [E.15] Alteración accidental de la información	5	1	1	7	3	MODERADO	4	FRECUENTE
	5.3.11. [E.18] Destrucción de información	4	3	5	12	4	ALTO	2	POCO FRECUENTE
	5.3.12. [E.19] Fugas de información	1	5	2	8	3	MODERADO	2	POCO FRECUENTE
5.4. [A] Ataques intencionados	5.4.3. [A.5] Suplantación de la identidad del usuario	5	5	1	11	4	ALTO	3	NORMAL
	5.4.4. [A.6] Abuso de privilegios de acceso	5	5	5	15	5	MUY ALTO	4	FRECUENTE
	5.4.9. [A.11] Acceso no autorizado	5	5	1	11	4	ALTO	3	NORMAL
	5.4.13. [A.15] Modificación deliberada de la información	5	3	2	10	4	ALTO	3	NORMAL
	5.4.15. [A.19] Divulgación de información	4	5	1	10	4	ALTO	4	FRECUENTE

- **INFORMACIÓN: [INFO_PER]**

Tabla E.2. Matriz de identificación y valoración de amenazas [INFO_PER]

[INFO] INFORMACIÓN									
[INFO_PER]	**Base de datos de clientes y proveedores**								
TIPO DE AMENAZAS	**AMENAZAS**	**Dv: DEGRADACIÓN DE VALOR POR DIMENSIONES**						**PROBABILIDAD DE OCURRENCIA**	
		Dv-i	**Dv-c**	**Dv-d**	**Dt-ex**	**DT**	**NIVEL**	**Po**	**NIVEL**
5.3. [E] Errores y fallos no intencionados	5.3.1. [E.1] Errores de los usuarios	4	4	4	12	4	ALTO	5	MUY FRECUENTE
	5.3.2. [E.2] Errores del administrador	5	5	5	15	5	MUY ALTO	5	MUY FRECUENTE
	5.3.10. [E.15] Alteración accidental de la información	5	4	4	13	5	MUY ALTO	3	NORMAL
	5.3.11. [E.18] Destrucción de información	3	5	5	13	5	MUY ALTO	3	NORMAL
	5.3.12. [E.19] Fugas de información	5	5	4	14	5	MUY ALTO	4	FRECUENTE
5.4. [A] Ataques intencionados	5.4.3. [A.5] Suplantación de la identidad del usuario	5	5	1	11	4	ALTO	3	NORMAL
	5.4.4. [A.6] Abuso de privilegios de acceso	3	3	5	11	4	ALTO	2	POCO FRECUENTE
	5.4.9. [A.11] Acceso no autorizado	4	5	3	12	4	ALTO	3	NORMAL
	5.4.13. [A.15] Modificación deliberada de la información	5	4	2	11	4	ALTO	2	POCO FRECUENTE
	5.4.15. [A.19] Divulgación de información	4	5	1	10	4	ALTO	4	FRECUENTE

- **INFORMACIÓN: [INFO_PUB]**

Tabla E.3. Matriz de identificación y valoración de amenazas [INFO_PUB]

[INFO] INFORMACIÓN									
[INFO_PUB]	**Documentación y permisos de funcionamiento**								
TIPO DE AMENAZAS	**AMENAZAS**	**Dv: DEGRADACIÓN DE VALOR POR DIMENSIONES**						**PROBABILIDAD DE OCURRENCIA**	
		Dv-i	**Dv-c**	**Dv-d**	**Dt-ex**	**DT**	**NIVEL**	**Po**	**NIVEL**
5.3. [E] Errores y fallos no intencionados	5.3.1. [E.1] Errores de los usuarios	4	4	5	13	5	MUY ALTO	5	MUY FRECUENTE
	5.3.2. [E.2] Errores del administrador	5	5	5	15	5	MUY ALTO	5	MUY FRECUENTE
	5.3.10. [E.15] Alteración accidental de la información	5	1	5	11	4	ALTO	4	FRECUENTE
	5.3.11. [E.18] Destrucción de información	5	5	5	15	5	MUY ALTO	2	POCO FRECUENTE
	5.3.12. [E.19] Fugas de información	2	5	5	12	4	ALTO	2	POCO FRECUENTE
5.4. [A] Ataques intencionados	5.4.3. [A.5] Suplantación de la identidad del usuario	3	3	1	7	3	MODERADO	3	NORMAL
	5.4.4. [A.6] Abuso de privilegios de acceso	2	2	1	5	5	MUY ALTO	3	NORMAL
	5.4.9. [A.11] Acceso no autorizado	3	2	2	7	3	MODERADO	3	NORMAL
	5.4.13. [A.15] Modificación deliberada de la información	5	3	2	10	4	ALTO	3	NORMAL
	5.4.15. [A.19] Divulgación de información	4	4	4	12	4	ALTO	4	FRECUENTE

- **DATOS E INFORMACIÓN COMPLEMENTARIA: [D_BCK]**

Tabla E.4. Matriz de identificación y valoración de amenazas [D_BCK]

[DI] DATOS E INFORMACIÓN COMPLEMENTARIA									
[D_BCK]	**Copias de seguridad *OwnCloud***								
TIPO DE AMENAZAS	**AMENAZAS**	**Dv: DEGRADACIÓN DE VALOR POR DIMENSIONES**						**PROBABILIDAD DE OCURRENCIA**	
		Dv-i	**Dv-c**	**Dv-d**	**Dt-ex**	**DT**	**NIVEL**	**Po**	**NIVEL**
5.3. [E] Errores y fallos no intencionados	5.3.1. [E.1] Errores de los usuarios	5	5	5	15	5	MUY ALTO	2	POCO FRECUENTE
	5.3.2. [E.2] Errores del administrador	5	5	5	15	5	MUY ALTO	4	FRECUENTE
	5.3.10. [E.15] Alteración accidental de la información	5	4	3	12	4	ALTO	3	NORMAL
	5.3.11. [E.18] Destrucción de información	2	3	5	10	4	ALTO	2	POCO FRECUENTE
	5.3.12. [E.19] Fugas de información	4	5	2	11	4	ALTO	2	POCO FRECUENTE
5.4. [A] Ataques intencionados	5.4.3. [A.5] Suplantación de la identidad del usuario	5	5	3	13	5	MUY ALTO	3	NORMAL
	5.4.4. [A.6] Abuso de privilegios de acceso	5	5	5	15	5	MUY ALTO	3	NORMAL
	5.4.9. [A.11] Acceso no autorizado	5	5	4	14	5	MUY ALTO	3	NORMAL
	5.4.13. [A.15] Modificación deliberada de la información	5	3	3	11	4	ALTO	3	NORMAL
	5.4.15. [A.19] Divulgación de información	3	5	4	12	4	ALTO	4	FRECUENTE

- **DATOS E INFORMACIÓN COMPLEMENTARIA: [D_LG]**

Tabla E.5. Matriz de identificación y valoración de amenazas [D_LG]

[DI] DATOS E INFORMACIÓN COMPLEMENTARIA									
[D_LG]	**Logs de SACI**								
TIPO DE AMENAZAS	**AMENAZAS**	**Dv: DEGRADACIÓN DE VALOR POR DIMENSIONES**						**PROBABILIDAD DE OCURRENCIA**	
		Dv-i	**Dv-c**	**Dv-d**	**Dt-ex**	**DT**	**NIVEL**	**Po**	**NIVEL**
5.3. [E] Errores y fallos no intencionados	5.3.1. [E.1] Errores de los usuarios	5	5	5	15	5	MUY ALTO	3	NORMAL
	5.3.2. [E.2] Errores del administrador	5	5	5	15	5	MUY ALTO	4	FRECUENTE
	5.3.3. [E.3] Errores de monitorización (log)	5	5	2	12	4	ALTO	4	FRECUENTE
	5.3.10. [E.15] Alteración accidental de la información	4	5	3	12	4	ALTO	3	NORMAL
	5.3.11. [E.18] Destrucción de información	2	5	5	12	4	ALTO	2	POCO FRECUENTE
	5.3.12. [E.19] Fugas de información	5	5	3	13	5	MUY ALTO	4	FRECUENTE
5.4. [A] Ataques intencionados	5.4.1. [A.3] Manipulación de los registros de actividad (log)	5	3	3	11	4	ALTO	2	POCO FRECUENTE
	5.4.3. [A.5] Suplantación de la identidad del usuario	5	4	3	12	4	ALTO	3	NORMAL
	5.4.4. [A.6] Abuso de privilegios de acceso	5	5	5	15	5	MUY ALTO	3	NORMAL
	5.4.9. [A.11] Acceso no autorizado	4	5	2	11	4	ALTO	2	POCO FRECUENTE
	5.4.13. [A.15] Modificación deliberada de la información	5	3	2	10	4	ALTO	3	NORMAL
	5.4.15. [A.19] Divulgación de información	3	5	3	11	4	ALTO	4	FRECUENTE

- **CLAVES CRIPTOGRÁFICAS: [K_PB]**

Tabla E.6. Matriz de identificación y valoración de amenazas [K_PB]

[K] CLAVES CRIPTOGRÁFICAS									
[K_PB]	**SSL**								
TIPO DE AMENAZAS	**AMENAZAS**	**Dv: DEGRADACIÓN DE VALOR POR DIMENSIONES**						**PROBABILIDAD DE OCURRENCIA**	
		Dv-i	**Dv-c**	**Dv-d**	**Dt-ex**	**DT**	**NIVEL**	**Po**	**NIVEL**
5.3. [E] Errores y fallos no intencionados	5.3.1. [E.1] Errores de los usuarios	5	5	5	15	5	MUY ALTO	2	POCO FRECUENTE
	5.3.2. [E.2] Errores del administrador	5	5	5	15	5	MUY ALTO	4	FRECUENTE
	5.3.10. [E.15] Alteración accidental de la información	5	3	1	9	3	MODERADO	3	NORMAL
	5.3.11. [E.18] Destrucción de información	1	2	5	8	3	MODERADO	2	POCO FRECUENTE
	5.3.12. [E.19] Fugas de información	1	5	3	9	3	MODERADO	3	NORMAL
5.4. [A] Ataques intencionados	5.4.3. [A.5] Suplantación de la identidad del usuario	5	5	5	15	5	MUY ALTO	2	POCO FRECUENTE
	5.4.4. [A.6] Abuso de privilegios de acceso	5	5	5	15	5	MUY ALTO	2	POCO FRECUENTE
	5.4.9. [A.11] Acceso no autorizado	5	5	4	14	5	MUY ALTO	3	NORMAL
	5.4.13. [A.15] Modificación deliberada de la información	5	4	3	12	4	ALTO	2	POCO FRECUENTE
	5.4.15. [A.19] Divulgación de información	1	5	1	7	3	MODERADO	2	POCO FRECUENTE

- **CLAVES CRIPTOGRÁFICAS: [K_SIGN]**

Tabla E.7. Matriz de identificación y valoración de amenazas [K_SIGN]

[K] CLAVES CRIPTOGRÁFICAS									
[K_SIGN]	**Token Digital**								
TIPO DE AMENAZAS	**AMENAZAS**	**Dv: DEGRADACIÓN DE VALOR POR DIMENSIONES**						**PROBABILIDAD DE OCURRENCIA**	
		Dv-i	**Dv-c**	**Dv-d**	**Dt-ex**	**DT**	**NIVEL**	**Po**	**NIVEL**
5.3. [E] Errores y fallos no intencionados	5.3.1. [E.1] Errores de los usuarios	3	5	3	11	4	ALTO	3	NORMAL
	5.3.2. [E.2] Errores del administrador	5	5	5	15	5	MUY ALTO	4	FRECUENTE
	5.3.10. [E.15] Alteración accidental de la información	5	4	5	14	5	MUY ALTO	4	FRECUENTE
	5.3.11. [E.18] Destrucción de información	4	3	5	12	4	ALTO	2	POCO FRECUENTE
	5.3.12. [E.19] Fugas de información	3	5	3	11	4	ALTO	2	POCO FRECUENTE
5.4. [A] Ataques intencionados	5.4.3. [A.5] Suplantación de la identidad del usuario	5	5	4	14	5	MUY ALTO	3	NORMAL
	5.4.4. [A.6] Abuso de privilegios de acceso	5	5	3	13	5	MUY ALTO	2	POCO FRECUENTE
	5.4.9. [A.11] Acceso no autorizado	5	5	2	12	4	ALTO	3	NORMAL
	5.4.13. [A.15] Modificación deliberada de la información	5	5	3	13	5	MUY ALTO	2	POCO FRECUENTE
	5.4.15. [A.19] Divulgación de información	5	5	3	13	5	MUY ALTO	2	POCO FRECUENTE

- **SERVICIOS [S_INT]**

Tabla E.8. Matriz de identificación y valoración de amenazas [S_INT]

[S] SERVICIOS									
[S_INT]	**Servicio del sistema contable**								
TIPO DE AMENAZAS	**AMENAZAS**	**Dv: DEGRADACIÓN DE VALOR POR DIMENSIONES**						**PROBABILIDAD DE OCURRENCIA**	
		Dv-i	**Dv-c**	**Dv-d**	**Dt-ex**	**DT**	**NIVEL**	**Po**	**NIVEL**
5.3. [E] Errores y fallos no intencionados	5.3.1. [E.1] Errores de los usuarios	5	5	4	14	5	MUY ALTO	5	MUY FRECUENTE
	5.3.2. [E.2] Errores del administrador	5	5	5	15	5	MUY ALTO	5	MUY FRECUENTE
	5.3.10. [E.15] Alteración accidental de la información	5	3	1	9	3	MODERADO	4	FRECUENTE
	5.3.11. [E.18] Destrucción de información	2	3	5	10	4	ALTO	2	POCO FRECUENTE
	5.3.12. [E.19] Fugas de información	1	5	2	8	3	MODERADO	4	FRECUENTE
5.4. [A] Ataques intencionados	5.4.3. [A.5] Suplantación de la identidad del usuario	5	5	3	13	5	MUY ALTO	4	FRECUENTE
	5.4.4. [A.6] Abuso de privilegios de acceso	5	5	5	15	5	MUY ALTO	2	POCO FRECUENTE
	5.4.9. [A.11] Acceso no autorizado	5	5	1	11	4	ALTO	3	NORMAL
	5.4.13. [A.15] Modificación deliberada de la información	5	3	2	10	4	ALTO	2	POCO FRECUENTE
	5.4.15. [A.19] Divulgación de información	2	5	2	9	3	MODERADO	4	FRECUENTE
	5.4.18. [A.24] Denegación de servicio	2	4	5	11	4	ALTO	5	MUY FRECUENTE

- **SERVICIOS [S_WWW]**

Tabla E.9. Matriz de identificación y valoración de amenazas [S_WWW]

[S] SERVICIOS									
[S_WWW]	**Sitio web**								
TIPO DE AMENAZAS	**AMENAZAS**	**Dv: DEGRADACIÓN DE VALOR POR DIMENSIONES**						**PROBABILIDAD DE OCURRENCIA**	
		Dv-i	**Dv-c**	**Dv-d**	**Dt-ex**	**DT**	**NIVEL**	**Po**	**NIVEL**
5.3. [E] Errores y fallos no intencionados	5.3.1. [E.1] Errores de los usuarios	5	5	5	15	5	MUY ALTO	5	MUY FRECUENTE
	5.3.2. [E.2] Errores del administrador	5	5	5	15	5	MUY ALTO	4	FRECUENTE
	5.3.10. [E.15] Alteración accidental de la información	4	5	3	12	4	ALTO	4	FRECUENTE
	5.3.11. [E.18] Destrucción de información	2	5	5	12	4	ALTO	2	POCO FRECUENTE
	5.3.12. [E.19] Fugas de información	2	5	4	11	4	ALTO	4	FRECUENTE
5.4. [A] Ataques intencionados	5.4.3. [A.5] Suplantación de la identidad del usuario	5	5	4	14	5	MUY ALTO	4	FRECUENTE
	5.4.4. [A.6] Abuso de privilegios de acceso	5	5	5	15	5	MUY ALTO	2	POCO FRECUENTE
	5.4.9. [A.11] Acceso no autorizado	5	5	3	13	5	MUY ALTO	3	NORMAL
	5.4.13. [A.15] Modificación deliberada de la información	5	4	2	11	4	ALTO	2	POCO FRECUENTE
	5.4.15. [A.19] Divulgación de información	2	5	1	8	3	MODERADO	4	FRECUENTE
	5.4.18. [A.24] Denegación de servicio	1	4	5	10	4	ALTO	2	POCO FRECUENTE

- **SOFTWARE- APLICACIONES INFORMÁTICAS: [SW_HP]**

Tabla E.10. Matriz de identificación y valoración de amenazas [SW_HP]

[SW] SOFTWARE- APLICACIONES INFORMÁTICAS									
[SW_HP]	**Proxmox**								
TIPO DE AMENAZAS	**AMENAZAS**	**Dv: DEGRADACIÓN DE VALOR POR DIMENSIONES**						**PROBABILIDAD DE OCURRENCIA**	
		Dv-i	**Dv-c**	**Dv-d**	**Dt-ex**	**DT**	**NIVEL**	**Po**	**NIVEL**
5.2. [I] De origen industrial	5.2.6. [I.5] Avería de origen físico o lógico	1	4	5	10	4	ALTO	5	MUY FRECUENTE
5.3. [E] Errores y fallos no intencionados	5.3.1. [E.1] Errores de los usuarios	5	5	5	15	5	MUY ALTO	3	NORMAL
	5.3.2. [E.2] Errores del administrador	5	5	5	15	5	MUY ALTO	2	POCO FRECUENTE
	5.3.6. [E.8] Difusión de software dañino	5	5	5	15	5	MUY ALTO	3	NORMAL
	5.3.10. [E.15] Alteración accidental de la información	5	4	4	13	5	MUY ALTO	2	POCO FRECUENTE
	5.3.11. [E.18] Destrucción de información	3	4	5	12	4	ALTO	2	POCO FRECUENTE
	5.3.12. [E.19] Fugas de información	2	5	5	12	4	ALTO	3	NORMAL
	5.3.13. [E.20] Vulnerabilidades de los programas (software)	5	5	5	15	5	MUY ALTO	5	MUY FRECUENTE
	5.3.14. [E.21] Errores de mantenimiento / actualización de programas (software)	5	3	5	13	5	MUY ALTO	5	MUY FRECUENTE
5.4. [A] Ataques intencionados	5.4.3. [A.5] Suplantación de la identidad del usuario	5	5	4	14	5	MUY ALTO	2	POCO FRECUENTE
	5.4.4. [A.6] Abuso de privilegios de acceso	5	5	5	15	5	MUY ALTO	4	FRECUENTE
	5.4.9. [A.11] Acceso no autorizado	5	5	2	12	4	ALTO	3	NORMAL
	5.4.13. [A.15] Modificación deliberada de la información	5	4	3	12	4	ALTO	3	NORMAL
	5.4.15. [A.19] Divulgación de información	1	5	2	8	3	MODERADO	3	NORMAL
	5.4.16. [A.22] Manipulación de programas	5	5	5	15	5	MUY ALTO	4	FRECUENTE
	5.4.18. [A.24] Denegación de servicio	1	4	5	10	4	ALTO	2	POCO FRECUENTE

- **SOFTWARE- APLICACIONES INFORMÁTICAS: [SW_BD1]**

Tabla E.11. Matriz de identificación y valoración de amenazas [SW_BD1]

[SW] SOFTWARE- APLICACIONES INFORMÁTICAS									
[SW_BD1]	**Servidor de Base de Datos Oracle XE 18c**								
TIPO DE AMENAZAS	**AMENAZAS**	**Dv: DEGRADACIÓN DE VALOR POR DIMENSIONES**						**PROBABILIDAD DE OCURRENCIA**	
		Dv-i	**Dv-c**	**Dv-d**	**Dt-ex**	**DT**	**NIVEL**	**Po**	**NIVEL**
5.2. [I] De origen industrial	5.2.6. [I.5] Avería de origen físico o lógico	4	4	5	13	5	MUY ALTO	2	POCO FRECUENTE
5.3. [E] Errores y fallos no intencionados	5.3.1. [E.1] Errores de los usuarios	5	5	5	15	5	MUY ALTO	5	MUY FRECUENTE
	5.3.2. [E.2] Errores del administrador	5	5	5	15	5	MUY ALTO	5	MUY FRECUENTE
	5.3.6. [E.8] Difusión de software dañino	5	5	5	15	5	MUY ALTO	3	NORMAL
	5.3.10. [E.15] Alteración accidental de la información	5	3	4	12	4	ALTO	2	POCO FRECUENTE
	5.3.11. [E.18] Destrucción de información	2	4	5	11	4	ALTO	2	POCO FRECUENTE
	5.3.12. [E.19] Fugas de información	2	5	2	9	3	MODERADO	3	NORMAL
5.4. [A] Ataques intencionados	5.4.3. [A.5] Suplantación de la identidad del usuario	5	5	4	14	5	MUY ALTO	2	POCO FRECUENTE
	5.4.9. [A.11] Acceso no autorizado	5	5	2	12	4	ALTO	2	POCO FRECUENTE
	5.4.13. [A.15] Modificación deliberada de la información	5	4	3	12	4	ALTO	3	NORMAL
	5.4.15. [A.19] Divulgación de información	2	5	2	9	3	MODERADO	4	FRECUENTE
	5.4.18. [A.24] Denegación de servicio	2	4	5	11	4	ALTO	2	POCO FRECUENTE

- **SOFTWARE- APLICACIONES INFORMÁTICAS: [SW_APP4]**

Tabla E.12. Matriz de identificación y valoración de amenazas [SW_APP4]

[SW] SOFTWARE- APLICACIONES INFORMÁTICAS									
[SW_APP4]	**Servidor Digital Ocean**								
TIPO DE AMENAZAS	**AMENAZAS**	**Dv: DEGRADACIÓN DE VALOR POR DIMENSIONES**						**PROBABILIDAD DE OCURRENCIA**	
		Dv-i	**Dv-c**	**Dv-d**	**Dt-ex**	**DT**	**NIVEL**	**Po**	**NIVEL**
5.2. [I] De origen industrial	5.2.6. [I.5] Avería de origen físico o lógico	2	5	5	12	4	ALTO	3	NORMAL
5.3. [E] Errores y fallos no intencionados	5.3.2. [E.2] Errores del administrador	3	5	5	13	5	MUY ALTO	4	FRECUENTE
	5.3.6. [E.8] Difusión de software dañino	3	5	5	13	5	MUY ALTO	3	NORMAL
5.4. [A] Ataques intencionados	5.4.3. [A.5] Suplantación de la identidad del usuario	3	5	3	11	4	ALTO	2	POCO FRECUENTE
	5.4.4. [A.6] Abuso de privilegios de acceso	3	4	5	12	4	ALTO	4	FRECUENTE
	5.4.9. [A.11] Acceso no autorizado	2	5	3	10	4	ALTO	3	NORMAL

- **SOFTWARE- APLICACIONES INFORMÁTICAS: [SW_APP2]**

Tabla E.13. Matriz de identificación y valoración de amenazas [SW_APP2]

[SW] SOFTWARE- APLICACIONES INFORMÁTICAS									
[SW_APP2]	**Servidor FTP**								
TIPO DE AMENAZAS	**AMENAZAS**	**Dv: DEGRADACIÓN DE VALOR POR DIMENSIONES**						**PROBABILIDAD DE OCURRENCIA**	
		Dv-i	**Dv-c**	**Dv-d**	**Dt-ex**	**DT**	**NIVEL**	**Po**	**NIVEL**
5.2. [I] De origen industrial	5.2.6. [I.5] Avería de origen físico o lógico	3	3	2	8	3	MODERADO	4	FRECUENTE
5.3. [E] Errores y fallos no intencionados	5.3.2. [E.2] Errores del administrador	3	3	1	7	3	MODERADO	5	MUY FRECUENTE
	5.3.6. [E.8] Difusión de software dañino	3	5	5	13	5	MUY ALTO	3	NORMAL
	5.3.10. [E.15] Alteración accidental de la información	5	3	1	9	3	MODERADO	2	POCO FRECUENTE
	5.3.11. [E.18] Destrucción de información	3	3	5	11	4	ALTO	1	MUY POCO FRECUENTE
5.4. [A] Ataques intencionados	5.4.3. [A.5] Suplantación de la identidad del usuario	4	5	2	11	4	ALTO	2	POCO FRECUENTE
	5.4.4. [A.6] Abuso de privilegios de acceso	5	5	5	15	5	MUY ALTO	4	FRECUENTE
	5.4.9. [A.11] Acceso no autorizado	5	5	3	13	5	MUY ALTO	3	NORMAL
	5.4.18. [A.24] Denegación de servicio	2	4	5	11	4	ALTO	1	MUY POCO FRECUENTE

- **SOFTWARE- APLICACIONES INFORMÁTICAS: [SW_BD2]**

Tabla E.14. Matriz de identificación y valoración de amenazas [SW_BD2]

[SW] SOFTWARE- APLICACIONES INFORMÁTICAS									
[SW_BD2]	**Servidor de Base de Datos MySQL 8.0**								
TIPO DE AMENAZAS	**AMENAZAS**	**Dv: DEGRADACIÓN DE VALOR POR DIMENSIONES**						**PROBABILIDAD DE OCURRENCIA**	
		Dv-i	**Dv-c**	**Dv-d**	**Dt-ex**	**DT**	**NIVEL**	**Po**	**NIVEL**
5.2. [I] De origen industrial	5.2.6. [I.5] Avería de origen físico o lógico	4	4	5	13	5	MUY ALTO	3	NORMAL
5.3. [E] Errores y fallos no intencionados	5.3.1. [E.1] Errores de los usuarios	5	5	3	13	5	MUY ALTO	4	FRECUENTE
	5.3.2. [E.2] Errores del administrador	5	5	5	15	5	MUY ALTO	5	MUY FRECUENTE
	5.3.6. [E.8] Difusión de software dañino	3	5	5	13	5	MUY ALTO	3	NORMAL
	5.3.10. [E.15] Alteración accidental de la información	5	5	3	13	5	MUY ALTO	2	POCO FRECUENTE
	5.3.11. [E.18] Destrucción de información	2	3	5	10	4	ALTO	1	MUY POCO FRECUENTE
	5.3.12. [E.19] Fugas de información	1	5	2	8	3	MODERADO	3	NORMAL
	5.4.3. [A.5] Suplantación de la identidad del usuario	2	5	4	11	4	ALTO	2	POCO FRECUENTE
5.4. [A] Ataques intencionados	5.4.9. [A.11] Acceso no autorizado	4	5	2	11	4	ALTO	4	FRECUENTE
	5.4.13. [A.15] Modificación deliberada de la información	5	5	3	13	5	MUY ALTO	3	NORMAL
	5.4.15. [A.19] Divulgación de información	1	5	2	8	3	MODERADO	4	FRECUENTE
	5.4.18. [A.24] Denegación de servicio	2	3	5	10	4	ALTO	2	POCO FRECUENTE

- **SOFTWARE- APLICACIONES INFORMÁTICAS: [SW_APP3]**

Tabla E.15. Matriz de identificación y valoración de amenazas [SW_APP3]

[SW] SOFTWARE- APLICACIONES INFORMÁTICAS									
[SW_APP3]	**Servidor DNS**								
TIPO DE AMENAZAS	**AMENAZAS**	**Dv: DEGRADACIÓN DE VALOR POR DIMENSIONES**						**PROBABILIDAD DE OCURRENCIA**	
		Dv-i	**Dv-c**	**Dv-d**	**Dt-ex**	**DT**	**NIVEL**	**Po**	**NIVEL**
5.2. [I] De origen industrial	5.2.6. [I.5] Avería de origen físico o lógico	3	4	5	12	4	ALTO	3	NORMAL
5.3. [E] Errores y fallos no intencionados	5.3.2. [E.2] Errores del administrador	5	5	5	15	5	MUY ALTO	4	FRECUENTE
	5.3.6. [E.8] Difusión de software dañino	1	5	5	11	4	ALTO	3	NORMAL
5.4. [A] Ataques intencionados	5.4.3. [A.5] Suplantación de la identidad del usuario	4	5	3	12	4	ALTO	2	POCO FRECUENTE
	5.4.4. [A.6] Abuso de privilegios de acceso	5	5	5	15	5	MUY ALTO	4	FRECUENTE
	5.4.9. [A.11] Acceso no autorizado	5	5	3	13	5	MUY ALTO	3	NORMAL
	5.4.18. [A.24] Denegación de servicio	2	5	5	12	4	ALTO	2	POCO FRECUENTE

- **SOFTWARE- APLICACIONES INFORMÁTICAS: [SW_BD3]**

Tabla E.16. Matriz de identificación y valoración de amenazas [SW_BD3]

[SW] SOFTWARE- APLICACIONES INFORMÁTICAS									
[SW_BD3]	**Servidor de Base de Datos Postgresql 13**								
TIPO DE AMENAZAS	**AMENAZAS**	**Dv: DEGRADACIÓN DE VALOR POR DIMENSIONES**						**PROBABILIDAD DE OCURRENCIA**	
		Dv-i	**Dv-c**	**Dv-d**	**Dt-ex**	**DT**	**NIVEL**	**Po**	**NIVEL**
5.2. [I] De origen industrial	5.2.6. [I.5] Avería de origen físico o lógico	1	4	5	10	4	ALTO	3	NORMAL
5.3. [E] Errores y fallos no intencionados	5.3.1. [E.1] Errores de los usuarios	5	5	5	15	5	MUY ALTO	4	FRECUENTE
	5.3.2. [E.2] Errores del administrador	5	5	5	15	5	MUY ALTO	5	MUY FRECUENTE
	5.3.6. [E.8] Difusión de software dañino	4	3	5	12	4	ALTO	3	NORMAL
	5.3.10. [E.15] Alteración accidental de la información	5	5	3	13	5	MUY ALTO	4	FRECUENTE
	5.3.11. [E.18] Destrucción de información	1	4	5	10	4	ALTO	2	POCO FRECUENTE
	5.3.12. [E.19] Fugas de información	2	5	3	10	4	ALTO	4	FRECUENTE
	5.4.3. [A.5] Suplantación de la identidad del usuario	2	5	2	9	3	MODERADO	2	POCO FRECUENTE
5.4. [A] Ataques intencionados	5.4.9. [A.11] Acceso no autorizado	3	5	2	10	4	ALTO	3	NORMAL
	5.4.13. [A.15] Modificación deliberada de la información	5	4	2	11	4	ALTO	3	NORMAL
	5.4.15. [A.19] Divulgación de información	1	5	2	8	3	MODERADO	4	FRECUENTE
	5.4.18. [A.24] Denegación de servicio	2	3	5	10	4	ALTO	2	POCO FRECUENTE

- **SOFTWARE- APLICACIONES INFORMÁTICAS: [SW_AV]**

Tabla E.17. Matriz de identificación y valoración de amenazas [SW_AV]

[SW] SOFTWARE- APLICACIONES INFORMÁTICAS									
[SW_AV]	**Avast Free Antivirus**								
TIPO DE AMENAZAS	**AMENAZAS**	**Dv: DEGRADACIÓN DE VALOR POR DIMENSIONES**						**PROBABILIDAD DE OCURRENCIA**	
		Dv-i	**Dv-c**	**Dv-d**	**Dt-ex**	**DT**	**NIVEL**	**Po**	**NIVEL**
5.2. [I] De origen industrial	5.2.6. [I.5] Avería de origen físico o lógico	2	5	5	12	4	ALTO	3	NORMAL
5.3. [E] Errores y fallos no intencionados	5.3.1. [E.1] Errores de los usuarios	3	5	5	13	5	MUY ALTO	4	FRECUENTE
	5.3.2. [E.2] Errores del administrador	3	5	5	13	5	MUY ALTO	4	FRECUENTE
	5.3.6. [E.8] Difusión de software dañino	5	5	5	15	5	MUY ALTO	4	FRECUENTE
	5.3.13. [E.20] Vulnerabilidades de los programas (software)	2	5	5	12	4	ALTO	5	MUY FRECUENTE
	5.3.14. [E.21] Errores de mantenimiento / actualización de programas (software)	2	5	5	12	4	ALTO	5	MUY FRECUENTE
5.4. [A] Ataques intencionados	5.4.3. [A.5] Suplantación de la identidad del usuario	5	5	5	15	5	MUY ALTO	3	NORMAL
	5.4.4. [A.6] Abuso de privilegios de acceso	5	5	5	15	5	MUY ALTO	4	FRECUENTE
	5.4.9. [A.11] Acceso no autorizado	3	5	2	10	4	ALTO	3	NORMAL

- **SOFTWARE- APLICACIONES INFORMÁTICAS: [SW_APP1]**

Tabla E.18. Matriz de identificación y valoración de amenazas [SW_APP1]

[SW] SOFTWARE- APLICACIONES INFORMÁTICAS									
[SW_APP1]	**Servidor de OwnCloud**								
TIPO DE AMENAZAS	**AMENAZAS**	**Dv: DEGRADACIÓN DE VALOR POR DIMENSIONES**						**PROBABILIDAD DE OCURRENCIA**	
		Dv-i	**Dv-c**	**Dv-d**	**Dt-ex**	**DT**	**NIVEL**	**Po**	**NIVEL**
5.2. [I] De origen industrial	5.2.6. [I.5] Avería de origen físico o lógico	5	5	5	15	5	MUY ALTO	3	NORMAL
5.3. [E] Errores y fallos no intencionados	5.3.1. [E.1] Errores de los usuarios	5	5	2	12	4	ALTO	5	MUY FRECUENTE
	5.3.2. [E.2] Errores del administrador	5	5	5	15	5	MUY ALTO	5	MUY FRECUENTE
	5.3.6. [E.8] Difusión de software dañino	5	5	5	15	5	MUY ALTO	3	NORMAL
	5.3.10. [E.15] Alteración accidental de la información	5	5	4	14	5	MUY ALTO	3	NORMAL
	5.3.11. [E.18] Destrucción de información	2	4	5	11	4	ALTO	1	MUY POCO FRECUENTE
	5.3.12. [E.19] Fugas de información	2	5	3	10	4	ALTO	5	MUY FRECUENTE
	5.3.14. [E.21] Errores de mantenimiento / actualización de programas (software)	2	5	5	12	4	ALTO	5	MUY FRECUENTE
5.4. [A] Ataques intencionados	5.4.3. [A.5] Suplantación de la identidad del usuario	4	5	3	12	4	ALTO	3	NORMAL
	5.4.4. [A.6] Abuso de privilegios de acceso	5	5	5	15	5	MUY ALTO	4	FRECUENTE
	5.4.9. [A.11] Acceso no autorizado	5	5	2	12	4	ALTO	3	NORMAL
	5.4.13. [A.15] Modificación deliberada de la información	5	5	3	13	5	MUY ALTO	3	NORMAL
	5.4.15. [A.19] Divulgación de información	1	5	1	7	3	MODERADO	5	MUY FRECUENTE
	5.4.18. [A.24] Denegación de servicio	1	5	5	11	4	ALTO	1	MUY POCO FRECUENTE

- **SOFTWARE- APLICACIONES INFORMÁTICAS: [SW_WWW]**

Tabla E.19. Matriz de identificación y valoración de amenazas [SW_WWW]

[SW] SOFTWARE- APLICACIONES INFORMÁTICAS									
[SW_WWW]	**Servidor Web NGINX**								
TIPO DE AMENAZAS	**AMENAZAS**	**Dv: DEGRADACIÓN DE VALOR POR DIMENSIONES**						**PROBABILIDAD DE OCURRENCIA**	
		Dv-i	**Dv-c**	**Dv-d**	**Dt-ex**	**DT**	**NIVEL**	**Po**	**NIVEL**
5.2. [I] De origen industrial	5.2.6. [I.5] Avería de origen físico o lógico	2	2	5	9	3	MODERADO	3	NORMAL
5.3. [E] Errores y fallos no intencionados	5.3.2. [E.2] Errores del administrador	3	4	5	12	4	ALTO	5	MUY FRECUENTE
	5.3.6. [E.8] Difusión de software dañino	4	5	5	14	5	MUY ALTO	3	NORMAL
5.4. [A] Ataques intencionados	5.4.3. [A.5] Suplantación de la identidad del usuario	2	5	3	10	4	ALTO	1	MUY POCO FRECUENTE
	5.4.4. [A.6] Abuso de privilegios de acceso	4	5	4	13	5	MUY ALTO	4	FRECUENTE
	5.4.9. [A.11] Acceso no autorizado	4	5	3	12	4	ALTO	3	NORMAL
	5.4.18. [A.24] Denegación de servicio	2	5	5	12	4	ALTO	1	MUY POCO FRECUENTE

- **SOFTWARE- APLICACIONES INFORMÁTICAS: [SW_OS]**

Tabla E.20. Matriz de identificación y valoración de amenazas [SW_OS]

[SW] SOFTWARE- APLICACIONES INFORMÁTICAS									
[SW_OS]	**Windows/Linux**								
TIPO DE AMENAZAS	**AMENAZAS**	**Dv: DEGRADACIÓN DE VALOR POR DIMENSIONES**						**PROBABILIDAD DE OCURRENCIA**	
		Dv-i	**Dv-c**	**Dv-d**	**Dt-ex**	**DT**	**NIVEL**	**Po**	**NIVEL**
5.2. [I] De origen industrial	5.2.6. [I.5] Avería de origen físico o lógico	1	3	5	9	3	MODERADO	4	FRECUENTE
5.3. [E] Errores y fallos no intencionados	5.3.1. [E.1] Errores de los usuarios	5	5	5	15	5	MUY ALTO	4	FRECUENTE
	5.3.2. [E.2] Errores del administrador	5	5	5	15	5	MUY ALTO	4	FRECUENTE
	5.3.6. [E.8] Difusión de software dañino	2	3	5	10	4	ALTO	3	NORMAL
	5.3.10. [E.15] Alteración accidental de la información	2	3	4	9	3	MODERADO	2	POCO FRECUENTE
	5.3.11. [E.18] Destrucción de información	1	4	5	10	4	ALTO	1	MUY POCO FRECUENTE
	5.3.12. [E.19] Fugas de información	2	5	3	10	4	ALTO	5	MUY FRECUENTE
	5.3.13. [E.20] Vulnerabilidades de los programas (software)	5	5	5	15	5	MUY ALTO	5	MUY FRECUENTE
	5.3.14. [E.21] Errores de mantenimiento / actualización de programas (software)	5	5	5	15	5	MUY ALTO	5	MUY FRECUENTE
5.4. [A] Ataques intencionados	5.4.3. [A.5] Suplantación de la identidad del usuario	1	5	4	10	4	ALTO	2	POCO FRECUENTE
	5.4.4. [A.6] Abuso de privilegios de acceso	1	5	5	11	4	ALTO	4	FRECUENTE
	5.4.9. [A.11] Acceso no autorizado	2	5	2	9	3	MODERADO	3	NORMAL
	5.4.13. [A.15] Modificación deliberada de la información	4	4	3	11	4	ALTO	3	NORMAL
	5.4.15. [A.19] Divulgación de información	1	5	2	8	3	MODERADO	5	MUY FRECUENTE
	5.4.18. [A.24] Denegación de servicio	1	4	5	10	4	ALTO	2	POCO FRECUENTE

- **SOFTWARE- APLICACIONES INFORMÁTICAS: [SW_ALM]**

Tabla E.21. Matriz de identificación y valoración de amenazas [SW_ALM]

[SW] SOFTWARE- APLICACIONES INFORMÁTICAS									
[SW_ALM]	**Google Drive**								
TIPO DE AMENAZAS	**AMENAZAS**	**Dv: DEGRADACIÓN DE VALOR POR DIMENSIONES**						**PROBABILIDAD DE OCURRENCIA**	
		Dv-i	**Dv-c**	**Dv-d**	**Dt-ex**	**DT**	**NIVEL**	**Po**	**NIVEL**
5.3. [E] Errores y fallos no intencionados	5.3.1. [E.1] Errores de los usuarios	3	4	4	11	4	ALTO	4	FRECUENTE
	5.3.2. [E.2] Errores del administrador	4	5	4	13	5	MUY ALTO	4	FRECUENTE
	5.3.10. [E.15] Alteración accidental de la información	5	4	4	13	5	MUY ALTO	3	NORMAL
	5.3.11. [E.18] Destrucción de información	1	5	5	11	4	ALTO	1	MUY POCO FRECUENTE
	5.3.12. [E.19] Fugas de información	5	5	5	15	5	MUY ALTO	5	MUY FRECUENTE
5.4. [A] Ataques intencionados	5.4.3. [A.5] Suplantación de la identidad del usuario	2	5	4	11	4	ALTO	3	NORMAL
	5.4.4. [A.6] Abuso de privilegios de acceso	4	5	3	12	4	ALTO	4	FRECUENTE
	5.4.9. [A.11] Acceso no autorizado	3	5	2	10	4	ALTO	3	NORMAL
	5.4.13. [A.15] Modificación deliberada de la información	5	5	2	12	4	ALTO	3	NORMAL
	5.4.15. [A.19] Divulgación de información	2	5	2	9	3	MODERADO	5	MUY FRECUENTE
	5.4.18. [A.24] Denegación de servicio	3	4	5	12	4	ALTO	2	POCO FRECUENTE

- **SOFTWARE- APLICACIONES INFORMÁTICAS: [SW_OFF]**

Tabla E.22. Matriz de identificación y valoración de amenazas [SW_OFF]

[SW] SOFTWARE- APLICACIONES INFORMÁTICAS									
[SW_OFF]	**Microsoft Office Professional 2019**								
TIPO DE AMENAZAS	**AMENAZAS**	**Dv: DEGRADACIÓN DE VALOR POR DIMENSIONES**						**PROBABILIDAD DE OCURRENCIA**	
		Dv-i	**Dv-c**	**Dv-d**	**Dt-ex**	**DT**	**NIVEL**	**Po**	**NIVEL**
5.2. [I] De origen industrial	5.2.6. [I.5] Avería de origen físico o lógico	1	5	5	11	4	ALTO	4	FRECUENTE
5.3. [E] Errores y fallos no intencionados	5.3.1. [E.1] Errores de los usuarios	3	5	5	13	5	MUY ALTO	3	NORMAL
	5.3.2. [E.2] Errores del administrador	3	5	5	13	5	MUY ALTO	3	NORMAL
	5.3.6. [E.8] Difusión de software dañino	5	5	5	15	5	MUY ALTO	3	NORMAL
	5.3.14. [E.21] Errores de mantenimiento / actualización de programas (software)	2	4	5	11	4	ALTO	3	NORMAL
5.4. [A] Ataques intencionados	5.4.3. [A.5] Suplantación de la identidad del usuario	2	5	4	11	4	ALTO	2	POCO FRECUENTE
	5.4.4. [A.6] Abuso de privilegios de acceso	4	5	3	12	4	ALTO	4	FRECUENTE
	5.4.9. [A.11] Acceso no autorizado	4	5	2	11	4	ALTO	3	NORMAL
	5.4.18. [A.24] Denegación de servicio	3	4	5	12	4	ALTO	2	POCO FRECUENTE

- **HARDWARE- EQUIPOS INFORMÁTICOS: [HW_HT]**

Tabla E.23. Matriz de identificación y valoración de amenazas [HW_HT]

[HW] HARDWARE- EQUIPOS INFORMÁTICOS									
[HW_HT]	**Servidor físico HP Proliant DL 360P**								
TIPO DE AMENAZAS	**AMENAZAS**	**Dv: DEGRADACIÓN DE VALOR POR DIMENSIONES**						**PROBABILIDAD DE OCURRENCIA**	
		Dv-i	**Dv-c**	**Dv-d**	**Dt-ex**	**DT**	**NIVEL**	**Po**	**NIVEL**
5.1. [N] Desastres naturales	5.1.1. [N.1] Fuego	3	4	5	12	4	ALTO	3	NORMAL
	5.1.2. [N.2] Daños por agua	3	4	5	12	4	ALTO	3	NORMAL
5.2. [I] De origen industrial	5.2.3. [I.*] Desastres industriales	3	4	5	12	4	ALTO	2	POCO FRECUENTE
	5.2.6. [I.5] Avería de origen físico o lógico	3	4	5	12	4	ALTO	3	NORMAL
	5.2.7. [I.6] Corte del suministro eléctrico	4	4	5	13	5	MUY ALTO	5	MUY FRECUENTE
5.3. [E] Errores y fallos no intencionados	5.3.2. [E.2] Errores del administrador	5	5	5	15	5	MUY ALTO	4	FRECUENTE
	5.3.15. [E.23] Errores de mantenimiento / actualización de equipos (hardware)	5	4	5	14	5	MUY ALTO	3	NORMAL
	5.3.17. [E.25] Pérdida de equipos	5	5	5	15	5	MUY ALTO	2	POCO FRECUENTE
5.4. [A] Ataques intencionados	5.4.4. [A.6] Abuso de privilegios de acceso	5	5	4	14	5	MUY ALTO	2	POCO FRECUENTE
	5.4.9. [A.11] Acceso no autorizado	4	5	2	11	4	ALTO	3	NORMAL
	5.4.17. [A.23] Manipulación de los equipos	5	5	5	15	5	MUY ALTO	2	POCO FRECUENTE
	5.4.19. [A.25] Robo	4	5	5	14	5	MUY ALTO	2	POCO FRECUENTE

- **HARDWARE- EQUIPOS INFORMÁTICOS: [HW_SW]**

Tabla E.24. Matriz de identificación y valoración de amenazas [HW_SW]

[HW] HARDWARE- EQUIPOS INFORMÁTICOS									
[HW_SW]	**Switch TP-LINK**								
TIPO DE AMENAZAS	**AMENAZAS**	**Dv: DEGRADACION DE VALOR POR DIMENSIONES**						**PROBABILIDAD DE OCURRENCIA**	
		Dv-i	**Dv-c**	**Dv-d**	**Dt-ex**	**DT**	**NIVEL**	**Po**	**NIVEL**
5.1. [N] Desastres naturales	5.1.1. [N.1] Fuego	3	5	5	13	5	MUY ALTO	3	NORMAL
	5.1.2. [N.2] Daños por agua	3	3	5	11	4	ALTO	3	NORMAL
5.2. [I] De origen industrial	5.2.3. [I.*] Desastres industriales	3	3	5	11	4	ALTO	2	POCO FRECUENTE
	5.2.6. [I.5] Avería de origen físico o lógico	5	3	5	13	5	MUY ALTO	3	NORMAL
	5.2.7. [I.6] Corte del suministro eléctrico	4	5	5	14	5	MUY ALTO	5	MUY FRECUENTE
5.3. [E] Errores y fallos no intencionados	5.3.2. [E.2] Errores del administrador	3	4	5	12	4	ALTO	4	FRECUENTE
	5.3.15. [E.23] Errores de mantenimiento / actualización de equipos (hardware)	3	4	5	12	4	ALTO	3	NORMAL
	5.3.17. [E.25] Pérdida de equipos	3	3	5	11	4	ALTO	2	POCO FRECUENTE
5.4. [A] Ataques intencionados	5.4.4. [A.6] Abuso de privilegios de acceso	5	3	3	11	4	ALTO	2	POCO FRECUENTE
	5.4.9. [A.11] Acceso no autorizado	4	5	3	12	4	ALTO	3	NORMAL
	5.4.17. [A.23] Manipulación de los equipos	5	5	2	12	4	ALTO	2	POCO FRECUENTE
	5.4.19. [A.25] Robo	3	5	5	13	5	MUY ALTO	2	POCO FRECUENTE

- **HARDWARE- EQUIPOS INFORMÁTICOS: [HW_MV2]**

Tabla E.25. Matriz de identificación y valoración de amenazas [HW_MV2]

[HW] HARDWARE- EQUIPOS INFORMÁTICOS									
[HW_MV2]	**Teléfonos móviles**								
TIPO DE AMENAZAS	**AMENAZAS**	**Dv: DEGRADACION DE VALOR POR DIMENSIONES**						**PROBABILIDAD DE OCURRENCIA**	
		Dv-i	**Dv-c**	**Dv-d**	**Dt-ex**	**DT**	**NIVEL**	**Po**	**NIVEL**
5.1. [N] Desastres naturales	5.1.1. [N.1] Fuego	3	5	5	13	5	MUY ALTO	3	NORMAL
	5.1.2. [N.2] Daños por agua	3	5	5	13	5	MUY ALTO	3	NORMAL
5.2. [I] De origen industrial	5.2.3. [I.*] Desastres industriales	3	5	5	13	5	MUY ALTO	2	POCO FRECUENTE
	5.2.6. [I.5] Avería de origen físico o lógico	2	4	5	11	4	ALTO	3	NORMAL
	5.2.7. [I.6] Corte del suministro eléctrico	2	3	4	9	3	MODERADO	4	FRECUENTE
5.3. [E] Errores y fallos no intencionados	5.3.1. [E.1] Errores de los usuarios	3	4	5	12	4	ALTO	5	MUY FRECUENTE
	5.3.2. [E.2] Errores del administrador	3	4	5	12	4	ALTO	5	MUY FRECUENTE
	5.3.12. [E.19] Fugas de información	5	5	5	15	5	MUY ALTO	5	MUY FRECUENTE
	5.3.15. [E.23] Errores de mantenimiento / actualización de equipos (hardware)	5	5	5	15	5	MUY ALTO	4	FRECUENTE
	5.3.17. [E.25] Pérdida de equipos	2	5	5	12	4	ALTO	4	FRECUENTE
	5.4.3. [A.5] Suplantación de la identidad del usuario	2	4	5	11	4	ALTO	3	NORMAL
5.4. [A] Ataques intencionados	5.4.4. [A.6] Abuso de privilegios de acceso	2	4	5	11	4	ALTO	3	NORMAL
	5.4.9. [A.11] Acceso no autorizado	3	5	3	11	4	ALTO	3	NORMAL
	5.4.17. [A.23] Manipulación de los equipos	3	4	5	12	4	ALTO	4	FRECUENTE
	5.4.19. [A.25] Robo	4	4	5	13	5	MUY ALTO	4	FRECUENTE

- **HARDWARE- EQUIPOS INFORMÁTICOS: [HW_PC]**

Tabla E.26. Matriz de identificación y valoración de amenazas [HW_PC]

[HW] HARDWARE- EQUIPOS INFORMÁTICOS									
[HW_PC]	**Computadoras de escritorio**								
TIPO DE AMENAZAS	**AMENAZAS**	**Dv: DEGRADACION DE VALOR POR DIMENSIONES**						**PROBABILIDAD DE OCURRENCIA**	
		Dv-i	**Dv-c**	**Dv-d**	**Dt-ex**	**DT**	**NIVEL**	**Po**	**NIVEL**
5.1. [N] Desastres naturales	5.1.1. [N.1] Fuego	1	2	5	8	3	MODERADO	3	NORMAL
	5.1.2. [N.2] Daños por agua	3	2	5	10	4	ALTO	3	NORMAL
5.2. [I] De origen industrial	5.2.3. [I.*] Desastres industriales	1	1	5	7	3	MODERADO	2	POCO FRECUENTE
	5.2.6. [I.5] Avería de origen físico o lógico	2	2	5	9	3	MODERADO	3	NORMAL
	5.2.7. [I.6] Corte del suministro eléctrico	3	5	5	13	5	MUY ALTO	4	FRECUENTE
5.3. [E] Errores y fallos no intencionados	5.3.1. [E.1] Errores de los usuarios	5	5	5	15	5	MUY ALTO	5	MUY FRECUENTE
	5.3.2. [E.2] Errores del administrador	5	5	5	15	5	MUY ALTO	5	MUY FRECUENTE
	5.3.15. [E.23] Errores de mantenimiento / actualización de equipos (hardware)	3	4	4	11	5	MUY ALTO	4	FRECUENTE
	5.3.17. [E.25] Pérdida de equipos	4	5	5	14	5	MUY ALTO	4	FRECUENTE
	5.4.3. [A.5] Suplantación de la identidad del usuario	4	5	4	13	5	MUY ALTO	3	NORMAL
5.4. [A] Ataques intencionados	5.4.4. [A.6] Abuso de privilegios de acceso	3	5	3	11	4	ALTO	3	NORMAL
	5.4.9. [A.11] Acceso no autorizado	4	5	3	12	4	ALTO	3	NORMAL
	5.4.17. [A.23] Manipulación de los equipos	4	5	3	12	4	ALTO	4	FRECUENTE
	5.4.19. [A.25] Robo	1	2	5	8	3	MODERADO	2	POCO FRECUENTE

- **HARDWARE- EQUIPOS INFORMÁTICOS: [HW_MV1]**

Tabla E.27. Matriz de identificación y valoración de amenazas [HW_MV1]

[HW] HARDWARE- EQUIPOS INFORMÁTICOS									
[HW_MV1]	**Computadoras Portátiles**								
TIPO DE AMENAZAS	**AMENAZAS**	**Dv: DEGRADACION DE VALOR POR DIMENSIONES**						**PROBABILIDAD DE OCURRENCIA**	
		Dv-i	**Dv-c**	**Dv-d**	**Dt-ex**	**DT**	**NIVEL**	**Po**	**NIVEL**
5.1. [N] Desastres naturales	5.1.1. [N.1] Fuego	2	2	5	9	3	MODERADO	3	NORMAL
	5.1.2. [N.2] Daños por agua	2	2	5	9	3	MODERADO	3	NORMAL
5.2. [I] De origen industrial	5.2.3. [I.*] Desastres industriales	1	2	5	8	3	MODERADO	2	POCO FRECUENTE
	5.2.6. [I.5] Avería de origen físico o lógico	2	4	5	11	4	ALTO	3	NORMAL
	5.2.7. [I.6] Corte del suministro eléctrico	5	5	5	15	5	MUY ALTO	5	MUY FRECUENTE
5.3. [E] Errores y fallos no intencionados	5.3.1. [E.1] Errores de los usuarios	5	5	2	12	4	ALTO	5	MUY FRECUENTE
	5.3.2. [E.2] Errores del administrador	5	5	3	13	5	MUY ALTO	5	MUY FRECUENTE
	5.3.15. [E.23] Errores de mantenimiento / actualización de equipos (hardware)	5	5	4	14	5	MUY ALTO	4	FRECUENTE
	5.3.17. [E.25] Pérdida de equipos	2	5	5	12	4	ALTO	4	FRECUENTE
	5.4.3. [A.5] Suplantación de la identidad del usuario	5	5	4	14	5	MUY ALTO	3	NORMAL
5.4. [A] Ataques intencionados	5.4.4. [A.6] Abuso de privilegios de acceso	5	5	3	13	5	MUY ALTO	3	NORMAL
	5.4.9. [A.11] Acceso no autorizado	3	5	3	11	4	ALTO	3	NORMAL
	5.4.17. [A.23] Manipulación de los equipos	3	5	3	11	4	ALTO	4	FRECUENTE
	5.4.19. [A.25] Robo	3	4	5	12	4	ALTO	4	FRECUENTE

- **HARDWARE- EQUIPOS INFORMÁTICOS: [HW_WAP]**

Tabla E.28. Matriz de identificación y valoración de amenazas [HW_WAP]

[HW] HARDWARE- EQUIPOS INFORMÁTICOS									
[HW_WAP]	**Puntos de Acceso**								
TIPO DE AMENAZAS	**AMENAZAS**	**Dv: DEGRADACION DE VALOR POR DIMENSIONES**						**PROBABILIDAD DE OCURRENCIA**	
		Dv-i	**Dv-c**	**Dv-d**	**Dt-ex**	**DT**	**NIVEL**	**Po**	**NIVEL**
5.1. [N] Desastres naturales	5.1.1. [N.1] Fuego	3	3	5	11	4	ALTO	2	POCO FRECUENTE
	5.1.2. [N.2] Daños por agua	3	3	5	11	4	ALTO	4	FRECUENTE
5.2. [I] De origen industrial	5.2.3. [I.*] Desastres industriales	3	3	5	11	4	ALTO	2	POCO FRECUENTE
	5.2.6. [I.5] Avería de origen físico o lógico	3	5	5	13	5	MUY ALTO	3	NORMAL
	5.2.7. [I.6] Corte del suministro eléctrico	5	5	5	15	5	MUY ALTO	5	MUY FRECUENTE
5.4. [A] Ataques intencionados	5.4.4. [A.6] Abuso de privilegios de acceso	3	5	3	11	5	MUY ALTO	3	NORMAL
	5.4.9. [A.11] Acceso no autorizado	5	4	3	12	4	ALTO	3	NORMAL
	5.4.17. [A.23] Manipulación de los equipos	5	5	3	13	5	MUY ALTO	3	NORMAL
	5.4.19. [A.25] Robo	5	5	5	15	5	MUY ALTO	2	POCO FRECUENTE

- **HARDWARE- EQUIPOS INFORMÁTICOS: [HW_PT]**

Tabla E.29. Matriz de identificación y valoración de amenazas [HW_PT]

[HW] HARDWARE- EQUIPOS INFORMÁTICOS									
[HW_PT]	**Impresoras**								
TIPO DE AMENAZAS	**AMENAZAS**	**Dv: DEGRADACION DE VALOR POR DIMENSIONES**						**PROBABILIDAD DE OCURRENCIA**	
		Dv-i	**Dv-c**	**Dv-d**	**Dt-ex**	**DT**	**NIVEL**	**Po**	**NIVEL**
5.1. [N] Desastres naturales	5.1.1. [N.1] Fuego	1	2	5	8	3	MODERADO	2	POCO FRECUENTE
	5.1.2. [N.2] Daños por agua	1	2	5	8	3	MODERADO	3	NORMAL
5.2. [I] De origen industrial	5.2.3. [I.*] Desastres industriales	1	1	4	6	2	BAJO	1	MUY POCO FRECUENTE
	5.2.6. [I.5] Avería de origen físico o lógico	1	3	5	9	3	MODERADO	3	NORMAL
	5.2.7. [I.6] Corte del suministro eléctrico	3	4	5	12	4	ALTO	5	MUY FRECUENTE
5.4. [A] Ataques intencionados	5.4.4. [A.6] Abuso de privilegios de acceso	2	5	3	10	4	ALTO	3	NORMAL
	5.4.9. [A.11] Acceso no autorizado	3	3	5	11	4	ALTO	3	NORMAL
	5.4.17. [A.23] Manipulación de los equipos	3	3	5	11	4	ALTO	3	NORMAL
	5.4.19. [A.25] Robo	1	3	5	9	3	MODERADO	1	MUY POCO FRECUENTE

- **REDES DE COMUNICACIONES: Internet Fibra Óptica**

Tabla E.30. Matriz de identificación y valoración de amenazas Internet Fibra Óptica

[COM] REDES DE COMUNICACIONES									
Internet Fibra Óptica	**Internet Fibra Óptica**								
TIPO DE AMENAZAS	**AMENAZAS**	**Dv: DEGRADACION DE VALOR POR DIMENSIONES**						**PROBABILIDAD DE OCURRENCIA**	
		Dv-i	**Dv-c**	**Dv-d**	**Dt-ex**	**DT**	**NIVEL**	**Po**	**NIVEL**
5.2. [I] De origen industrial	5.2.9. [I.8] Fallo de servicios de comunicaciones	2	4	5	11	4	ALTO	5	MUY FRECUENTE
5.3. [E] Errores y fallos no intencionados	5.3.2. [E.2] Errores del administrador	3	5	5	13	5	MUY ALTO	4	FRECUENTE
	5.3.11. [E.18] Destrucción de información	2	5	5	12	4	ALTO	2	POCO FRECUENTE
	5.3.12. [E.19] Fugas de información	2	5	5	12	4	ALTO	2	POCO FRECUENTE
5.4. [A] Ataques intencionados	5.4.3. [A.5] Suplantación de la identidad del usuario	3	5	3	11	4	ALTO	3	NORMAL
	5.4.4. [A.6] Abuso de privilegios de acceso	3	4	5	12	4	ALTO	3	NORMAL
	5.4.9. [A.11] Acceso no autorizado	2	5	4	11	4	ALTO	4	FRECUENTE
	5.4.10. [A.12] Análisis de tráfico	5	5	3	13	5	MUY ALTO	4	FRECUENTE
	5.4.13. [A.15] Modificación deliberada de la información	4	3	3	10	4	ALTO	2	POCO FRECUENTE
	5.4.15. [A.19] Divulgación de información	2	3	3	8	3	MODERADO	2	POCO FRECUENTE
	5.4.18. [A.24] Denegación de servicio	2	4	5	11	4	ALTO	3	NORMAL

- **REDES DE COMUNICACIONES: [COM_LAN]**

Tabla E.31. Matriz de identificación y valoración de amenazas [COM_LAN]

[COM] REDES DE COMUNICACIONES									
[COM_LAN]	**Red Local**								
TIPO DE AMENAZAS	**AMENAZAS**	**Dv: DEGRADACION DE VALOR POR DIMENSIONES**						**PROBABILIDAD DE OCURRENCIA**	
		Dv-i	**Dv-c**	**Dv-d**	**Dt-ex**	**DT**	**NIVEL**	**Po**	**NIVEL**
5.2. [I] De origen industrial	5.2.9. [I.8] Fallo de servicios de comunicaciones	4	5	5	14	5	MUY ALTO	5	MUY FRECUENTE
5.3. [E] Errores y fallos no intencionados	5.3.2. [E.2] Errores del administrador	5	5	5	15	5	MUY ALTO	4	FRECUENTE
	5.3.11. [E.18] Destrucción de información	3	5	4	12	4	ALTO	2	POCO FRECUENTE
	5.3.12. [E.19] Fugas de información	5	5	5	15	5	MUY ALTO	2	POCO FRECUENTE
5.4. [A] Ataques intencionados	5.4.3. [A.5] Suplantación de la identidad del usuario	3	5	3	11	4	ALTO	3	NORMAL
	5.4.4. [A.6] Abuso de privilegios de acceso	4	4	5	13	5	MUY ALTO	3	NORMAL
	5.4.9. [A.11] Acceso no autorizado	3	5	4	12	4	ALTO	4	FRECUENTE
	5.4.10. [A.12] Análisis de tráfico	5	5	5	15	5	MUY ALTO	4	FRECUENTE
	5.4.13. [A.15] Modificación deliberada de la información	5	5	5	15	5	MUY ALTO	3	NORMAL
	5.4.15. [A.19] Divulgación de información	3	5	3	11	4	ALTO	3	NORMAL
	5.4.18. [A.24] Denegación de servicio	3	4	5	12	4	ALTO	3	NORMAL

- **REDES DE COMUNICACIONES: [COM_MB]**

Tabla E.32. Matriz de identificación y valoración de amenazas [COM_MB]

[COM] REDES DE COMUNICACIONES									
[COM_MB]	**Telefonía Móvil**								
TIPO DE AMENAZAS	**AMENAZAS**	**Dv: DEGRADACION DE VALOR POR DIMENSIONES**						**PROBABILIDAD DE OCURRENCIA**	
		Dv-i	**Dv-c**	**Dv-d**	**Dt-ex**	**DT**	**NIVEL**	**Po**	**NIVEL**
5.2. [I] De origen industrial	5.2.9. [I.8] Fallo de servicios de comunicaciones	2	5	5	12	4	ALTO	5	MUY FRECUENTE
5.3. [E] Errores y fallos no intencionados	5.3.2. [E.2] Errores del administrador	2	5	5	12	4	ALTO	4	FRECUENTE
	5.3.11. [E.18] Destrucción de información	3	5	5	13	5	MUY ALTO	3	NORMAL
	5.3.12. [E.19] Fugas de información	5	5	5	15	5	MUY ALTO	5	MUY FRECUENTE
5.4. [A] Ataques intencionados	5.4.3. [A.5] Suplantación de la identidad del usuario	2	5	5	12	4	ALTO	2	POCO FRECUENTE
	5.4.4. [A.6] Abuso de privilegios de acceso	2	5	5	12	4	ALTO	3	NORMAL
	5.4.9. [A.11] Acceso no autorizado	2	5	4	11	4	ALTO	5	MUY FRECUENTE
	5.4.10. [A.12] Análisis de tráfico	2	5	3	10	4	ALTO	2	POCO FRECUENTE
	5.4.13. [A.15] Modificación deliberada de la información	3	5	3	11	4	ALTO	2	POCO FRECUENTE
	5.4.15. [A.19] Divulgación de información	5	5	3	13	5	MUY ALTO	5	MUY FRECUENTE
	5.4.18. [A.24] Denegación de servicio	3	5	5	13	5	MUY ALTO	3	NORMAL

- **REDES DE COMUNICACIONES: [COM_WF]**

Tabla E.33. Matriz de identificación y valoración de amenazas [COM_WF]

[COM] REDES DE COMUNICACIONES									
[COM_WF]	**Red Inalámbrica**								
TIPO DE AMENAZAS	**AMENAZAS**	**Dv: DEGRADACION DE VALOR POR DIMENSIONES**						**PROBABILIDAD DE OCURRENCIA**	
		Dv-i	**Dv-c**	**Dv-d**	**Dt-ex**	**DT**	**NIVEL**	**Po**	**NIVEL**
5.2. [I] De origen industrial	5.2.9. [I.8] Fallo de servicios de comunicaciones	2	5	5	12	4	ALTO	5	MUY FRECUENTE
5.3. [E] Errores y fallos no intencionados	5.3.2. [E.2] Errores del administrador	2	5	5	12	4	ALTO	4	FRECUENTE
	5.3.11. [E.18] Destrucción de información	1	1	5	7	3	MODERADO	3	NORMAL
	5.3.12. [E.19] Fugas de información	5	5	3	13	5	MUY ALTO	5	MUY FRECUENTE
5.4. [A] Ataques intencionados	5.4.3. [A.5] Suplantación de la identidad del usuario	3	4	2	9	3	MODERADO	3	NORMAL
	5.4.4. [A.6] Abuso de privilegios de acceso	3	5	3	11	4	ALTO	3	NORMAL
	5.4.9. [A.11] Acceso no autorizado	3	5	4	12	4	ALTO	4	FRECUENTE
	5.4.10. [A.12] Análisis de tráfico	3	5	3	11	4	ALTO	2	POCO FRECUENTE
	5.4.13. [A.15] Modificación deliberada de la información	5	3	2	10	4	ALTO	2	POCO FRECUENTE
	5.4.15. [A.19] Divulgación de información	5	5	3	13	5	MUY ALTO	4	FRECUENTE
	5.4.18. [A.24] Denegación de servicio	3	4	5	12	4	ALTO	3	NORMAL

- **EQUIPO AUXILIAR: [AUX_CB]**

Tabla E.34. Matriz de identificación y valoración de amenazas [AUX_CB]

[AUX] EQUIPO AUXILIAR									
[AUX_CB]	**Cableado Estructurado**								
TIPO DE AMENAZAS	**AMENAZAS**	**Dv: DEGRADACION DE VALOR POR DIMENSIONES**						**PROBABILIDAD DE OCURRENCIA**	
		Dv-i	**Dv-c**	**Dv-d**	**Dt-ex**	**DT**	**NIVEL**	**Po**	**NIVEL**
5.1. [N] Desastres naturales	5.1.1. [N.1] Fuego	2	2	5	9	3	MODERADO	2	POCO FRECUENTE
	5.1.2. [N.2] Daños por agua	2	3	5	10	4	ALTO	4	FRECUENTE
5.2. [I] De origen industrial	5.2.3. [I.*] Desastres industriales	2	2	5	9	3	MODERADO	2	POCO FRECUENTE
	5.2.4. [I.3] Contaminación mecánica	2	2	5	9	3	MODERADO	4	FRECUENTE
	5.2.6. [I.5] Avería de origen físico o lógico	3	3	5	11	4	ALTO	3	NORMAL
	5.2.7. [I.6] Corte del suministro eléctrico	3	2	5	10	4	ALTO	5	MUY FRECUENTE
	5.2.10. [I.9] Interrupción de otros servicios y suministros esenciales	2	3	5	10	4	ALTO	5	MUY FRECUENTE
5.3. [E] Errores y fallos no intencionados	5.3.15. [E.23] Errores de mantenimiento / actualización de equipos (hardware)	4	5	5	14	5	MUY ALTO	3	NORMAL
	5.3.17. [E.25] Pérdida de equipos	3	5	5	13	5	MUY ALTO	4	FRECUENTE
5.4. [A] Ataques intencionados	5.4.9. [A.11] Acceso no autorizado	2	5	3	10	4	ALTO	4	FRECUENTE
	5.4.17. [A.23] Manipulación de los equipos	4	4	5	13	5	MUY ALTO	4	FRECUENTE
	5.4.19. [A.25] Robo	3	5	5	13	5	MUY ALTO	2	POCO FRECUENTE

- **EQUIPO AUXILIAR: [AUX_VIDEO]**

Tabla E.35. Matriz de identificación y valoración de amenazas [AUX_VIDEO]

[AUX] EQUIPO AUXILIAR									
[AUX_VIDEO]	**Sistema de Video vigilancia**								
TIPO DE AMENAZAS	**AMENAZAS**	**Dv: DEGRADACION DE VALOR POR DIMENSIONES**						**PROBABILIDAD DE OCURRENCIA**	
		Dv-i	**Dv-c**	**Dv-d**	**Dt-ex**	**DT**	**NIVEL**	**Po**	**NIVEL**
5.1. [N] Desastres naturales	5.1.1. [N.1] Fuego	2	2	5	9	3	MODERADO	2	POCO FRECUENTE
	5.1.2. [N.2] Daños por agua	2	3	5	10	4	ALTO	4	FRECUENTE
5.2. [I] De origen industrial	5.2.3. [I.*] Desastres industriales	2	2	5	9	3	MODERADO	2	POCO FRECUENTE
	5.2.4. [I.3] Contaminación mecánica	2	2	5	9	3	MODERADO	4	FRECUENTE
	5.2.6. [I.5] Avería de origen físico o lógico	2	3	5	10	4	ALTO	3	NORMAL
	5.2.7. [I.6] Corte del suministro eléctrico	5	5	5	15	5	MUY ALTO	5	MUY FRECUENTE
	5.2.10. [I.9] Interrupción de otros servicios y suministros esenciales	3	3	5	11	4	ALTO	5	MUY FRECUENTE
5.3. [E] Errores y fallos no intencionados	5.3.15. [E.23] Errores de mantenimiento / actualización de equipos (hardware)	3	4	5	12	4	ALTO	3	NORMAL
	5.3.17. [E.25] Pérdida de equipos	1	3	5	9	3	MODERADO	4	FRECUENTE
5.4. [A] Ataques intencionados	5.4.9. [A.11] Acceso no autorizado	2	5	4	11	4	ALTO	4	FRECUENTE
	5.4.17. [A.23] Manipulación de los equipos	4	4	5	13	5	MUY ALTO	3	NORMAL
	5.4.19. [A.25] Robo	1	3	5	9	3	MODERADO	2	POCO FRECUENTE

- **EQUIPO AUXILIAR: [AUX_UPS]**

Tabla E.36. Matriz de identificación y valoración de amenazas [AUX_UPS]

[AUX] EQUIPO AUXILIAR									
[AUX_UPS]	**Sistema de alimentación Interrumpida**								
TIPO DE AMENAZAS	**AMENAZAS**	**Dv: DEGRADACION DE VALOR POR DIMENSIONES**						**PROBABILIDAD DE OCURRENCIA**	
		Dv-i	**Dv-c**	**Dv-d**	**Dt-ex**	**DT**	**NIVEL**	**Po**	**NIVEL**
5.1. [N] Desastres naturales	5.1.1. [N.1] Fuego	1	2	5	8	3	MODERADO	2	POCO FRECUENTE
	5.1.2. [N.2] Daños por agua	1	3	5	9	3	MODERADO	3	NORMAL
5.2. [I] De origen industrial	5.2.3. [I.*] Desastres industriales	1	2	5	8	3	MODERADO	2	POCO FRECUENTE
	5.2.4. [I.3] Contaminación mecánica	2	2	5	9	3	MODERADO	3	NORMAL
	5.2.6. [I.5] Avería de origen físico o lógico	2	3	5	10	4	ALTO	3	NORMAL
	5.2.7. [I.6] Corte del suministro eléctrico	5	5	5	15	5	MUY ALTO	4	FRECUENTE
5.3. [E] Errores y fallos no intencionados	5.3.15. [E.23] Errores de mantenimiento / actualización de equipos (hardware)	1	2	5	8	3	MODERADO	3	NORMAL
	5.3.17. [E.25] Pérdida de equipos	2	2	5	9	3	MODERADO	3	NORMAL
5.4. [A] Ataques intencionados	5.4.17. [A.23] Manipulación de los equipos	2	1	5	8	3	MODERADO	3	NORMAL
	5.4.19. [A.25] Robo	2	3	4	9	3	MODERADO	1	MUY POCO FRECUENTE

F. ANEXO F: VALORACIÓN DEL IMPACTO POTENCIAL

INFORMACIÓN: [INFO_VR]

Tabla F.1. Valoración del impacto potencial [INFO_VR]

[INFO] INFORMACIÓN					
[INFO_VR]	**Registros confidenciales de la organización**				
AMENAZAS	**IMPACTO POTENCIAL**				
	I: IMPACTO POTENCIAL POR DIMENSIONES			**IMPACTO TOTAL**	
	Ii	**Ic**	**Id**	**I-TOTAL**	**NIVEL**
5.3.1. [E.1] Errores de los usuarios	5	5	5	5	MUY ALTO
5.3.2. [E.2] Errores del administrador	5	5	5	5	MUY ALTO
5.3.10. [E.15] Alteración accidental de la información	5	1	1	3	MODERADO
5.3.11. [E.18] Destrucción de información	4	3	5	4	ALTO
5.3.12. [E.19] Fugas de información	1	5	2	3	MODERADO
5.4.3. [A.5] Suplantación de la identidad del usuario	5	5	1	4	ALTO
5.4.4. [A.6] Abuso de privilegios de acceso	5	5	5	5	MUY ALTO
5.4.9. [A.11] Acceso no autorizado	5	5	1	4	ALTO
5.4.13. [A.15] Modificación deliberada de la información	5	3	2	4	ALTO
5.4.15. [A.19] Divulgación de información	4	5	1	4	ALTO

- **INFORMACIÓN: [INFO_PER]**

Tabla F.2. Valoración del impacto potencial [INFO_PER]

[INFO] INFORMACIÓN					
[INFO_PER]	**Base de datos de clientes y proveedores**				
AMENAZAS	**IMPACTO POTENCIAL**				
	I: IMPACTO POTENCIAL POR DIMENSIONES			**IMPACTO TOTAL**	
	Ii	**Ic**	**Id**	**I-TOTAL**	**NIVEL**
5.3.1. [E.1] Errores de los usuarios	4	4	4	4	ALTO
5.3.2. [E.2] Errores del administrador	5	5	5	5	MUY ALTO
5.3.10. [E.15] Alteración accidental de la información	5	4	4	5	MUY ALTO
5.3.11. [E.18] Destrucción de información	3	5	5	5	MUY ALTO
5.3.12. [E.19] Fugas de información	5	5	4	5	MUY ALTO
5.4.3. [A.5] Suplantación de la identidad del usuario	5	5	1	4	ALTO
5.4.4. [A.6] Abuso de privilegios de acceso	3	3	5	4	ALTO
5.4.9. [A.11] Acceso no autorizado	4	5	3	4	ALTO
5.4.13. [A.15] Modificación deliberada de la información	5	4	2	4	ALTO
5.4.15. [A.19] Divulgación de información	4	5	1	4	ALTO

- **INFORMACIÓN: [INFO_PUB]**

Tabla F.3. Valoración del impacto potencial [INFO_PUB]

[INFO] INFORMACIÓN					
[INFO_PUB]	**Documentación y permisos de funcionamiento**				
AMENAZAS	**IMPACTO POTENCIAL**				
	I: IMPACTO POTENCIAL POR DIMENSIONES			**IMPACTO TOTAL**	
	Ii	**Ic**	**Id**	**I-TOTAL**	**NIVEL**
5.3.1. [E.1] Errores de los usuarios	4	4	5	5	MUY ALTO
5.3.2. [E.2] Errores del administrador	5	5	5	5	MUY ALTO
5.3.10. [E.15] Alteración accidental de la información	5	1	5	4	ALTO
5.3.11. [E.18] Destrucción de información	5	5	5	5	MUY ALTO
5.3.12. [E.19] Fugas de información	2	5	5	4	ALTO
5.4.3. [A.5] Suplantación de la identidad del usuario	3	3	1	3	MODERADO
5.4.4. [A.6] Abuso de privilegios de acceso	2	2	1	2	BAJO
5.4.9. [A.11] Acceso no autorizado	3	2	2	3	MODERADO
5.4.13. [A.15] Modificación deliberada de la información	5	3	2	4	ALTO
5.4.15. [A.19] Divulgación de información	4	4	4	4	ALTO

- **DATOS E INFORMACIÓN COMPLEMENTARIA: [D_BCK]**

Tabla F.4. Valoración del impacto potencial [D_BCK]

[DI] DATOS E INFORMACIÓN COMPLEMENTARIA					
[D_BCK]	**Copias de seguridad OwnCloud**				
AMENAZAS	**IMPACTO POTENCIAL**				
	I: IMPACTO POTENCIAL POR DIMENSIONES			**IMPACTO TOTAL**	
	Ii	**Ic**	**Id**	**I-TOTAL**	**NIVEL**
5.3.1. [E.1] Errores de los usuarios	5	5	5	5	MUY ALTO
5.3.2. [E.2] Errores del administrador	5	5	5	5	MUY ALTO
5.3.10. [E.15] Alteración accidental de la información	5	4	3	4	ALTO
5.3.11. [E.18] Destrucción de información	2	3	5	4	ALTO
5.3.12. [E.19] Fugas de información	4	5	2	4	ALTO
5.4.3. [A.5] Suplantación de la identidad del usuario	5	5	3	5	MUY ALTO
5.4.4. [A.6] Abuso de privilegios de acceso	5	5	5	5	MUY ALTO
5.4.9. [A.11] Acceso no autorizado	5	5	4	5	MUY ALTO
5.4.13. [A.15] Modificación deliberada de la información	5	3	3	4	ALTO
5.4.15. [A.19] Divulgación de información	3	5	4	4	ALTO

- **DATOS E INFORMACIÓN COMPLEMENTARIA: [D_LG]**

Tabla F.5. Valoración del impacto potencial [D_LG]

[DI] DATOS E INFORMACIÓN COMPLEMENTARIA					
[D_LG]	**Logs de SACI**				
AMENAZAS	**IMPACTO POTENCIAL**				
	I: IMPACTO POTENCIAL POR DIMENSIONES			**IMPACTO TOTAL**	
	Ii	**Ic**	**Id**	**I-TOTAL**	**NIVEL**
5.3.1. [E.1] Errores de los usuarios	4	4	4	4	ALTO
5.3.2. [E.2] Errores del administrador	4	4	4	4	ALTO
5.3.3. [E.3] Errores de monitorización (log)	4	4	2	4	ALTO
5.3.10. [E.15] Alteración accidental de la información	4	4	3	4	ALTO
5.3.11. [E.18] Destrucción de información	2	4	4	4	ALTO
5.3.12. [E.19] Fugas de información	4	4	3	4	ALTO
5.4.1. [A.3] Manipulación de los registros de actividad (log)	4	3	3	4	ALTO
5.4.3. [A.5] Suplantación de la identidad del usuario	4	4	3	4	ALTO
5.4.4. [A.6] Abuso de privilegios de acceso	4	4	4	4	ALTO
5.4.9. [A.11] Acceso no autorizado	4	4	2	4	ALTO
5.4.13. [A.15] Modificación deliberada de la información	4	3	2	3	MODERADO
5.4.15. [A.19] Divulgación de información	3	4	3	4	ALTO

- **CLAVES CRIPTOGRÁFICAS: [K_PB]**

Tabla F.6. Valoración del impacto potencial [K_PB]

[K] CLAVES CRIPTOGRÁFICAS					
[K_PB]	**SSL**				
AMENAZAS	**IMPACTO POTENCIAL**				
	I: IMPACTO POTENCIAL POR DIMENSIONES			**IMPACTO TOTAL**	
	Ii	**Ic**	**Id**	**I-TOTAL**	**NIVEL**
5.3.1. [E.1] Errores de los usuarios	5	5	5	5	MUY ALTO
5.3.2. [E.2] Errores del administrador	5	5	5	5	MUY ALTO
5.3.10. [E.15] Alteración accidental de la información	5	3	1	3	MODERADO
5.3.11. [E.18] Destrucción de información	1	2	5	3	MODERADO
5.3.12. [E.19] Fugas de información	1	5	3	3	MODERADO
5.4.3. [A.5] Suplantación de la identidad del usuario	5	5	5	5	MUY ALTO
5.4.4. [A.6] Abuso de privilegios de acceso	5	5	5	5	MUY ALTO
5.4.9. [A.11] Acceso no autorizado	5	5	4	5	MUY ALTO
5.4.13. [A.15] Modificación deliberada de la información	5	4	3	4	ALTO
5.4.15. [A.19] Divulgación de información	1	5	1	3	MODERADO

- **CLAVES CRIPTOGRÁFICAS: [K_SIGN]**

Tabla F.7. Valoración del impacto potencial [K_SIGN]

[K] CLAVES CRIPTOGRÁFICAS					
[K_SIGN]	**Token Digital**				
AMENAZAS	**IMPACTO POTENCIAL**				
	I: IMPACTO POTENCIAL POR DIMENSIONES			**IMPACTO TOTAL**	
	Ii	**Ic**	**Id**	**I-TOTAL**	**NIVEL**
5.3.1. [E.1] Errores de los usuarios	3	4	3	4	ALTO
5.3.2. [E.2] Errores del administrador	4	4	4	4	ALTO
5.3.10. [E.15] Alteración accidental de la información	4	4	4	4	ALTO
5.3.11. [E.18] Destrucción de información	4	3	4	4	ALTO
5.3.12. [E.19] Fugas de información	3	4	3	4	ALTO
5.4.3. [A.5] Suplantación de la identidad del usuario	4	4	4	4	ALTO
5.4.4. [A.6] Abuso de privilegios de acceso	4	4	3	4	ALTO
5.4.9. [A.11] Acceso no autorizado	4	4	2	4	ALTO
5.4.13. [A.15] Modificación deliberada de la información	4	4	3	4	ALTO
5.4.15. [A.19] Divulgación de información	4	4	3	4	ALTO

- **SERVICIOS: [S_INT]**

Tabla F.8. Valoración del impacto potencial [S_INT]

[S] SERVICIOS					
[S_INT]	**Servicio del sistema contable**				
AMENAZAS	**IMPACTO POTENCIAL**				
	I: IMPACTO POTENCIAL POR DIMENSIONES			**IMPACTO TOTAL**	
	Ii	**Ic**	**Id**	**I-TOTAL**	**NIVEL**
5.3.1. [E.1] Errores de los usuarios	5	5	4	5	MUY ALTO
5.3.2. [E.2] Errores del administrador	5	5	5	5	MUY ALTO
5.3.10. [E.15] Alteración accidental de la información	5	3	1	3	MODERADO
5.3.11. [E.18] Destrucción de información	2	3	5	4	ALTO
5.3.12. [E.19] Fugas de información	1	5	2	3	MODERADO
5.4.3. [A.5] Suplantación de la identidad del usuario	5	5	3	5	MUY ALTO
5.4.4. [A.6] Abuso de privilegios de acceso	5	5	5	5	MUY ALTO
5.4.9. [A.11] Acceso no autorizado	5	5	1	4	ALTO
5.4.13. [A.15] Modificación deliberada de la información	5	3	2	4	ALTO
5.4.15. [A.19] Divulgación de información	2	5	2	3	MODERADO

- **SERVICIOS: [S_WWW]**

Tabla F.9. Valoración del impacto potencial [S_WWW]

[S] SERVICIOS					
[S_WWW]	**Sitio web**				
AMENAZAS	**IMPACTO POTENCIAL**				
	I: IMPACTO POTENCIAL POR DIMENSIONES			**IMPACTO TOTAL**	
	Ii	**Ic**	**Id**	**I-TOTAL**	**NIVEL**
5.3.1. [E.1] Errores de los usuarios	4	4	4	4	ALTO
5.3.2. [E.2] Errores del administrador	4	4	4	4	ALTO
5.3.10. [E.15] Alteración accidental de la información	4	4	3	4	ALTO
5.3.11. [E.18] Destrucción de información	2	4	4	4	ALTO
5.3.12. [E.19] Fugas de información	2	4	4	4	ALTO
5.4.3. [A.5] Suplantación de la identidad del usuario	4	4	4	4	ALTO
5.4.4. [A.6] Abuso de privilegios de acceso	4	4	4	4	ALTO
5.4.9. [A.11] Acceso no autorizado	4	4	3	4	ALTO
5.4.13. [A.15] Modificación deliberada de la información	4	4	2	4	ALTO
5.4.15. [A.19] Divulgación de información	2	4	1	3	MODERADO
5.4.18. [A.24] Denegación de servicio	1	4	4	3	MODERADO

- **SOFTWARE- APLICACIONES INFORMÁTICAS: [SW_HP]**

Tabla F.10. Valoración del impacto potencial [SW_HP]

[SW] SOFTWARE- APLICACIONES INFORMÁTICAS					
[SW_HP]	**Proxmox**				
AMENAZAS	**IMPACTO POTENCIAL**				
	I: IMPACTO POTENCIAL POR DIMENSIONES			**IMPACTO TOTAL**	
	Ii	**Ic**	**Id**	**I-TOTAL**	**NIVEL**
5.2.6. [I.5] Avería de origen físico o lógico	1	4	5	4	ALTO
5.3.1. [E.1] Errores de los usuarios	5	5	5	5	MUY ALTO
5.3.2. [E.2] Errores del administrador	5	5	5	5	MUY ALTO
5.3.6. [E.8] Difusión de software dañino	5	5	5	5	MUY ALTO
5.3.10. [E.15] Alteración accidental de la información	5	4	4	5	MUY ALTO
5.3.11. [E.18] Destrucción de información	3	4	5	4	ALTO
5.3.12. [E.19] Fugas de información	2	5	5	4	ALTO
5.3.13. [E.20] Vulnerabilidades de los programas (software)	5	5	5	5	MUY ALTO
5.3.14. [E.21] Errores de mantenimiento / actualización de programas (software)	5	3	5	5	MUY ALTO
5.4.3. [A.5] Suplantación de la identidad del usuario	5	5	4	5	MUY ALTO
5.4.4. [A.6] Abuso de privilegios de acceso	5	5	5	5	MUY ALTO
5.4.9. [A.11] Acceso no autorizado	5	5	2	4	ALTO
5.4.13. [A.15] Modificación deliberada de la información	5	4	3	4	ALTO
5.4.15. [A.19] Divulgación de información	1	5	2	3	MODERADO
5.4.16. [A.22] Manipulación de programas	5	5	5	5	MUY ALTO
5.4.18. [A.24] Denegación de servicio	1	4	5	4	ALTO

- **SOFTWARE- APLICACIONES INFORMÁTICAS: [SW_BD1]**

Tabla F.11. Valoración del impacto potencial [SW_BD1]

[SW] SOFTWARE- APLICACIONES INFORMÁTICAS					
[SW_BD1]	**Servidor de Base de Datos Oracle XE 18c**				
AMENAZAS	**IMPACTO POTENCIAL**				
	I: IMPACTO POTENCIAL POR DIMENSIONES			**IMPACTO TOTAL**	
	Ii	**Ic**	**Id**	**I-TOTAL**	**NIVEL**
5.2.6. [I.5] Avería de origen físico o lógico	4	4	5	5	MUY ALTO
5.3.1. [E.1] Errores de los usuarios	5	5	5	5	MUY ALTO
5.3.2. [E.2] Errores del administrador	5	5	5	5	MUY ALTO
5.3.6. [E.8] Difusión de software dañino	5	5	5	5	MUY ALTO
5.3.10. [E.15] Alteración accidental de la información	5	3	4	4	ALTO
5.3.11. [E.18] Destrucción de información	2	4	5	4	ALTO
5.3.12. [E.19] Fugas de información	2	5	2	3	MODERADO
5.4.3. [A.5] Suplantación de la identidad del usuario	5	5	4	5	MUY ALTO
5.4.9. [A.11] Acceso no autorizado	5	5	2	4	ALTO
5.4.13. [A.15] Modificación deliberada de la información	5	4	3	4	ALTO
5.4.15. [A.19] Divulgación de información	2	5	2	3	MODERADO
5.4.18. [A.24] Denegación de servicio	2	4	5	4	ALTO

- **SOFTWARE- APLICACIONES INFORMÁTICAS: [SW_APP4]**

Tabla F.12. Valoración del impacto potencial [SW_APP4]

[SW] SOFTWARE- APLICACIONES INFORMÁTICAS					
[SW_APP4]	**Servidor Digital Ocean**				
AMENAZAS	**IMPACTO POTENCIAL**				
	I: IMPACTO POTENCIAL POR DIMENSIONES			**IMPACTO TOTAL**	
	Ii	**Ic**	**Id**	**I-TOTAL**	**NIVEL**
5.2.6. [I.5] Avería de origen físico o lógico	2	4	4	4	ALTO
5.3.2. [E.2] Errores del administrador	3	4	4	4	ALTO
5.3.6. [E.8] Difusión de software dañino	3	4	4	4	ALTO
5.4.3. [A.5] Suplantación de la identidad del usuario	3	4	3	4	ALTO
5.4.4. [A.6] Abuso de privilegios de acceso	3	4	4	4	ALTO
5.4.9. [A.11] Acceso no autorizado	2	4	3	3	MODERADO

- **SOFTWARE- APLICACIONES INFORMÁTICAS: [SW_APP2]**

Tabla F.13. Valoración del impacto potencial [SW_APP2]

[SW] SOFTWARE- APLICACIONES INFORMÁTICAS					
[SW_APP2]	**Servidor FTP**				
AMENAZAS	**IMPACTO POTENCIAL**				
	I: IMPACTO POTENCIAL POR DIMENSIONES			**IMPACTO TOTAL**	
	Ii	**Ic**	**Id**	**I-TOTAL**	**NIVEL**
5.2.6. [I.5] Avería de origen físico o lógico	3	3	2	3	MODERADO
5.3.2. [E.2] Errores del administrador	3	3	1	3	MODERADO
5.3.6. [E.8] Difusión de software dañino	3	4	4	4	ALTO
5.3.10. [E.15] Alteración accidental de la información	4	3	1	3	MODERADO
5.3.11. [E.18] Destrucción de información	3	3	4	4	ALTO
5.4.3. [A.5] Suplantación de la identidad del usuario	4	4	2	4	ALTO
5.4.4. [A.6] Abuso de privilegios de acceso	4	4	4	4	ALTO
5.4.9. [A.11] Acceso no autorizado	4	4	3	4	ALTO
5.4.18. [A.24] Denegación de servicio	2	4	4	4	ALTO

- **SOFTWARE- APLICACIONES INFORMÁTICAS: [SW_BD2]**

Tabla F.14. Valoración del impacto potencial [SW_BD2]

[SW] SOFTWARE- APLICACIONES INFORMÁTICAS					
[SW_BD2]	**Servidor de Base de Datos MySQL 8.0**				
AMENAZAS	**IMPACTO POTENCIAL**				
	I: IMPACTO POTENCIAL POR DIMENSIONES			**IMPACTO TOTAL**	
	Ii	**Ic**	**Id**	**I-TOTAL**	**NIVEL**
5.2.6. [I.5] Avería de origen físico o lógico	4	4	4	4	ALTO
5.3.1. [E.1] Errores de los usuarios	4	4	3	4	ALTO
5.3.2. [E.2] Errores del administrador	4	4	4	4	ALTO
5.3.6. [E.8] Difusión de software dañino	3	4	4	4	ALTO
5.3.10. [E.15] Alteración accidental de la información	4	4	3	4	ALTO
5.3.11. [E.18] Destrucción de información	2	3	4	3	MODERADO
5.3.12. [E.19] Fugas de información	1	4	2	3	MODERADO
5.4.3. [A.5] Suplantación de la identidad del usuario	2	4	4	4	ALTO
5.4.9. [A.11] Acceso no autorizado	4	4	2	4	ALTO
5.4.13. [A.15] Modificación deliberada de la información	4	4	3	4	ALTO
5.4.15. [A.19] Divulgación de información	1	4	2	3	MODERADO
5.4.18. [A.24] Denegación de servicio	2	3	4	3	MODERADO

- **SOFTWARE- APLICACIONES INFORMÁTICAS: [SW_APP3]**

Tabla F.15. Valoración del impacto potencial [SW_APP3]

[SW] SOFTWARE- APLICACIONES INFORMÁTICAS					
[SW_APP3]	**Servidor DNS**				
AMENAZAS	**IMPACTO POTENCIAL**				
	I: IMPACTO POTENCIAL POR DIMENSIONES			**IMPACTO TOTAL**	
	Ii	**Ic**	**Id**	**I-TOTAL**	**NIVEL**
5.2.6. [I.5] Avería de origen físico o lógico	3	4	4	4	ALTO
5.3.2. [E.2] Errores del administrador	4	4	4	4	ALTO
5.3.6. [E.8] Difusión de software dañino	1	4	4	3	MODERADO
5.4.3. [A.5] Suplantación de la identidad del usuario	4	4	3	4	ALTO
5.4.4. [A.6] Abuso de privilegios de acceso	4	4	4	4	ALTO
5.4.9. [A.11] Acceso no autorizado	4	4	3	4	ALTO
5.4.18. [A.24] Denegación de servicio	2	4	4	4	ALTO

- **SOFTWARE- APLICACIONES INFORMÁTICAS: [SW_BD3]**

Tabla F.16. Valoración del impacto potencial [SW_BD3]

[SW] SOFTWARE- APLICACIONES INFORMÁTICAS					
[SW_BD3]	Servidor de Base de Datos Postgresql 13				
AMENAZAS	IMPACTO POTENCIAL				
	I: IMPACTO POTENCIAL POR DIMENSIONES			IMPACTO TOTAL	
	Ii	Ic	Id	I-TOTAL	NIVEL
5.2.6. [I.5] Avería de origen físico o lógico	1	4	4	3	MODERADO
5.3.1. [E.1] Errores de los usuarios	4	4	4	4	ALTO
5.3.2. [E.2] Errores del administrador	4	4	4	4	ALTO
5.3.6. [E.8] Difusión de software dañino	4	3	4	4	ALTO
5.3.10. [E.15] Alteración accidental de la información	4	4	3	4	ALTO
5.3.11. [E.18] Destrucción de información	1	4	4	3	MODERADO
5.3.12. [E.19] Fugas de información	2	4	3	3	MODERADO
5.4.3. [A.5] Suplantación de la identidad del usuario	2	4	2	3	MODERADO
5.4.9. [A.11] Acceso no autorizado	3	4	2	3	MODERADO
5.4.13. [A.15] Modificación deliberada de la información	4	4	2	4	ALTO
5.4.15. [A.19] Divulgación de información	1	4	2	3	MODERADO
5.4.18. [A.24] Denegación de servicio	2	3	4	3	MODERADO

- **SOFTWARE- APLICACIONES INFORMÁTICAS: [SW_AV]**

Tabla F.17. Valoración del impacto potencial [SW_AV]

[SW] SOFTWARE- APLICACIONES INFORMÁTICAS					
[SW_AV]	**Avast Free Antivirus**				
AMENAZAS	**IMPACTO POTENCIAL**				
	I: IMPACTO POTENCIAL POR DIMENSIONES			**IMPACTO TOTAL**	
	Ii	**Ic**	**Id**	**I-TOTAL**	**NIVEL**
5.2.6. [I.5] Avería de origen físico o lógico	2	5	5	4	ALTO
5.3.1. [E.1] Errores de los usuarios	3	5	5	5	MUY ALTO
5.3.2. [E.2] Errores del administrador	3	5	5	5	MUY ALTO
5.3.6. [E.8] Difusión de software dañino	5	5	5	5	MUY ALTO
5.3.13. [E.20] Vulnerabilidades de los programas (software)	2	5	5	4	ALTO
5.3.14. [E.21] Errores de mantenimiento / actualización de programas (software)	2	5	5	4	ALTO
5.4.3. [A.5] Suplantación de la identidad del usuario	5	5	5	5	MUY ALTO
5.4.4. [A.6] Abuso de privilegios de acceso	5	5	5	5	MUY ALTO
5.4.9. [A.11] Acceso no autorizado	3	5	2	4	ALTO

- **SOFTWARE- APLICACIONES INFORMÁTICAS: [SW_APP1]**

Tabla F.18. Valoración del impacto potencial [SW_APP1]

[SW] SOFTWARE- APLICACIONES INFORMÁTICAS					
[SW_APP1]	**Servidor de OwnCloud**				
AMENAZAS	**IMPACTO POTENCIAL**				
	I: IMPACTO POTENCIAL POR DIMENSIONES			**IMPACTO TOTAL**	
	Ii	**Ic**	**Id**	**I-TOTAL**	**NIVEL**
5.2.6. [I.5] Avería de origen físico o lógico	4	4	4	4	ALTO
5.3.1. [E.1] Errores de los usuarios	4	4	2	4	ALTO
5.3.2. [E.2] Errores del administrador	4	4	4	4	ALTO
5.3.6. [E.8] Difusión de software dañino	4	4	4	4	ALTO
5.3.10. [E.15] Alteración accidental de la información	4	4	4	4	ALTO
5.3.11. [E.18] Destrucción de información	2	4	4	4	ALTO
5.3.12. [E.19] Fugas de información	2	4	3	3	MODERADO
5.3.14. [E.21] Errores de mantenimiento / actualización de programas (software)	2	4	4	4	ALTO
5.4.3. [A.5] Suplantación de la identidad del usuario	4	4	3	4	ALTO
5.4.4. [A.6] Abuso de privilegios de acceso	4	4	4	4	ALTO
5.4.9. [A.11] Acceso no autorizado	4	4	2	4	ALTO
5.4.13. [A.15] Modificación deliberada de la información	4	4	3	4	ALTO
5.4.15. [A.19] Divulgación de información	1	4	1	2	BAJO
5.4.18. [A.24] Denegación de servicio	1	4	4	3	MODERADO

- **SOFTWARE- APLICACIONES INFORMÁTICAS: [SW_WWW]**

Tabla F.19. Valoración del impacto potencial [SW_WWW]

[SW] SOFTWARE- APLICACIONES INFORMÁTICAS					
[SW_WWW]	**Servidor Web NGINX**				
AMENAZAS	**IMPACTO POTENCIAL**				
	I: IMPACTO POTENCIAL POR DIMENSIONES			**IMPACTO TOTAL**	
	Ii	**Ic**	**Id**	**I-TOTAL**	**NIVEL**
5.2.6. [I.5] Avería de origen físico o lógico	2	2	3	3	MODERADO
5.3.2. [E.2] Errores del administrador	2	3	3	3	MODERADO
5.3.6. [E.8] Difusión de software dañino	3	3	3	3	MODERADO
5.4.3. [A.5] Suplantación de la identidad del usuario	2	3	2	3	MODERADO
5.4.4. [A.6] Abuso de privilegios de acceso	3	3	3	3	MODERADO
5.4.9. [A.11] Acceso no autorizado	3	3	2	3	MODERADO
5.4.18. [A.24] Denegación de servicio	2	3	3	3	MODERADO

- **SOFTWARE- APLICACIONES INFORMÁTICAS: [SW_OS]**

Tabla F.20. Valoración del impacto potencial [SW_OS]

[SW] SOFTWARE- APLICACIONES INFORMÁTICAS					
[SW_OS]	**Windows/Linux**				
AMENAZAS	**IMPACTO POTENCIAL**				
	I: IMPACTO POTENCIAL POR DIMENSIONES			**IMPACTO TOTAL**	
	Ii	**Ic**	**Id**	**I-TOTAL**	**NIVEL**
5.2.6. [I.5] Avería de origen físico o lógico	1	3	4	3	MODERADO
5.3.1. [E.1] Errores de los usuarios	4	4	4	4	ALTO
5.3.2. [E.2] Errores del administrador	4	4	4	4	ALTO
5.3.6. [E.8] Difusión de software dañino	2	3	4	3	MODERADO
5.3.10. [E.15] Alteración accidental de la información	2	3	4	3	MODERADO
5.3.11. [E.18] Destrucción de información	1	4	4	3	MODERADO
5.3.12. [E.19] Fugas de información	2	4	3	3	MODERADO
5.3.13. [E.20] Vulnerabilidades de los programas (software)	4	4	4	4	ALTO
5.3.14. [E.21] Errores de mantenimiento / actualización de programas (software)	4	4	4	4	ALTO
5.4.3. [A.5] Suplantación de la identidad del usuario	1	4	4	3	MODERADO
5.4.4. [A.6] Abuso de privilegios de acceso	1	4	4	3	MODERADO
5.4.9. [A.11] Acceso no autorizado	2	4	2	3	MODERADO
5.4.13. [A.15] Modificación deliberada de la información	4	4	3	4	ALTO
5.4.15. [A.19] Divulgación de información	1	4	2	3	MODERADO
5.4.18. [A.24] Denegación de servicio	1	4	4	3	MODERADO

- **SOFTWARE- APLICACIONES INFORMÁTICAS: [SW_ALM]**

Tabla F.21. Valoración del impacto potencial [SW_ALM]

[SW] SOFTWARE- APLICACIONES INFORMÁTICAS					
[SW_ALM]	**Google Drive**				
AMENAZAS	**IMPACTO POTENCIAL**				
	I: IMPACTO POTENCIAL POR DIMENSIONES			**IMPACTO TOTAL**	
	Ii	**Ic**	**Id**	**I-TOTAL**	**NIVEL**
5.3.1. [E.1] Errores de los usuarios	2	3	3	3	MODERADO
5.3.2. [E.2] Errores del administrador	3	3	3	3	MODERADO
5.3.10. [E.15] Alteración accidental de la información	3	3	3	3	MODERADO
5.3.11. [E.18] Destrucción de información	1	3	3	3	MODERADO
5.3.12. [E.19] Fugas de información	3	3	3	3	MODERADO
5.4.3. [A.5] Suplantación de la identidad del usuario	2	3	3	3	MODERADO
5.4.4. [A.6] Abuso de privilegios de acceso	3	3	2	3	MODERADO
5.4.9. [A.11] Acceso no autorizado	2	3	2	3	MODERADO
5.4.13. [A.15] Modificación deliberada de la información	3	3	2	3	MODERADO
5.4.15. [A.19] Divulgación de información	2	3	2	3	MODERADO
5.4.18. [A.24] Denegación de servicio	2	3	3	3	MODERADO

- **SOFTWARE- APLICACIONES INFORMÁTICAS: [SW_OFF]**

Tabla F.22. Valoración del impacto potencial [SW_OFF]

[SW] SOFTWARE- APLICACIONES INFORMÁTICAS					
[SW_OFF]	**Microsoft Office Professional 2019**				
AMENAZAS	**IMPACTO POTENCIAL**				
	I: IMPACTO POTENCIAL POR DIMENSIONES			**IMPACTO TOTAL**	
	Ii	**Ic**	**Id**	**I-TOTAL**	**NIVEL**
5.2.6. [I.5] Avería de origen físico o lógico	1	3	3	3	MODERADO
5.3.1. [E.1] Errores de los usuarios	2	3	3	3	MODERADO
5.3.2. [E.2] Errores del administrador	2	3	3	3	MODERADO
5.3.6. [E.8] Difusión de software dañino	3	3	3	3	MODERADO
5.3.14. [E.21] Errores de mantenimiento / actualización de programas (software)	2	3	3	3	MODERADO
5.4.3. [A.5] Suplantación de la identidad del usuario	2	3	3	3	MODERADO
5.4.4. [A.6] Abuso de privilegios de acceso	3	3	2	3	MODERADO
5.4.9. [A.11] Acceso no autorizado	3	3	2	3	MODERADO
5.4.18. [A.24] Denegación de servicio	2	3	3	3	MODERADO

- **HARDWARE- EQUIPOS INFORMÁTICOS: [HW_HT]**

Tabla F.23. Valoración del impacto potencial [HW_HT]

[HW] HARDWARE- EQUIPOS INFORMÁTICOS					
[HW_HT]	**Servidor físico HP Proliant DL 360P**				
AMENAZAS	**IMPACTO POTENCIAL**				
	I: IMPACTO POTENCIAL POR DIMENSIONES			**IMPACTO TOTAL**	
	Ii	**Ic**	**Id**	**I-TOTAL**	**NIVEL**
5.1.1. [N.1] Fuego	3	4	5	4	ALTO
5.1.2. [N.2] Daños por agua	3	4	5	4	ALTO
5.2.3. [I.*] Desastres industriales	3	4	5	4	ALTO
5.2.6. [I.5] Avería de origen físico o lógico	3	4	5	4	ALTO
5.2.7. [I.6] Corte del suministro eléctrico	4	4	5	5	MUY ALTO
5.3.2. [E.2] Errores del administrador	5	5	5	5	MUY ALTO
5.3.15. [E.23] Errores de mantenimiento / actualización de equipos (hardware)	5	4	5	5	MUY ALTO
5.3.17. [E.25] Pérdida de equipos	5	5	5	5	MUY ALTO
5.4.4. [A.6] Abuso de privilegios de acceso	5	5	4	5	MUY ALTO
5.4.9. [A.11] Acceso no autorizado	4	5	2	4	ALTO
5.4.17. [A.23] Manipulación de los equipos	5	5	5	5	MUY ALTO
5.4.19. [A.25] Robo	4	5	5	5	MUY ALTO

- **HARDWARE- EQUIPOS INFORMÁTICOS: [HW_SW]**

Tabla F.24. Valoración del impacto potencial [HW_SW]

[HW] HARDWARE- EQUIPOS INFORMÁTICOS					
[HW_SW]	**Switch TP-LINK**				
AMENAZAS	**IMPACTO POTENCIAL**				
	I: IMPACTO POTENCIAL POR DIMENSIONES			**IMPACTO TOTAL**	
	Ii	**Ic**	**Id**	**I-TOTAL**	**NIVEL**
5.1.1. [N.1] Fuego	3	5	5	5	MUY ALTO
5.1.2. [N.2] Daños por agua	3	3	5	4	ALTO
5.2.3. [I.*] Desastres industriales	3	3	5	4	ALTO
5.2.6. [I.5] Avería de origen físico o lógico	5	3	5	5	MUY ALTO
5.2.7. [I.6] Corte del suministro eléctrico	4	5	5	5	MUY ALTO
5.3.2. [E.2] Errores del administrador	3	4	5	4	ALTO
5.3.15. [E.23] Errores de mantenimiento / actualización de equipos (hardware)	3	4	5	4	ALTO
5.3.17. [E.25] Pérdida de equipos	3	3	5	4	ALTO
5.4.4. [A.6] Abuso de privilegios de acceso	5	3	3	4	ALTO
5.4.9. [A.11] Acceso no autorizado	4	5	3	4	ALTO
5.4.17. [A.23] Manipulación de los equipos	5	5	2	4	ALTO
5.4.19. [A.25] Robo	4	5	5	5	MUY ALTO

- **HARDWARE- EQUIPOS INFORMÁTICOS: [HW_MV2]**

Tabla F.25. Valoración del impacto potencial [HW_MV2]

[HW] HARDWARE- EQUIPOS INFORMÁTICOS					
[HW_MV2]	**Teléfonos móviles**				
AMENAZAS	**IMPACTO POTENCIAL**				
	I: IMPACTO POTENCIAL POR DIMENSIONES			**IMPACTO TOTAL**	
	Ii	**Ic**	**Id**	**I-TOTAL**	**NIVEL**
5.1.1. [N.1] Fuego	3	5	5	5	MUY ALTO
5.1.2. [N.2] Daños por agua	3	5	5	5	MUY ALTO
5.2.3. [I.*] Desastres industriales	3	5	5	5	MUY ALTO
5.2.6. [I.5] Avería de origen físico o lógico	2	4	5	4	ALTO
5.2.7. [I.6] Corte del suministro eléctrico	2	3	4	3	MODERADO
5.3.1. [E.1] Errores de los usuarios	3	4	5	4	ALTO
5.3.2. [E.2] Errores del administrador	3	4	5	4	ALTO
5.3.12. [E.19] Fugas de información	5	5	5	5	MUY ALTO
5.3.15. [E.23] Errores de mantenimiento / actualización de equipos (hardware)	5	5	5	5	MUY ALTO
5.3.17. [E.25] Pérdida de equipos	2	5	5	4	ALTO
5.4.3. [A.5] Suplantación de la identidad del usuario	2	4	5	4	ALTO
5.4.4. [A.6] Abuso de privilegios de acceso	2	4	5	4	ALTO
5.4.9. [A.11] Acceso no autorizado	3	5	3	4	ALTO
5.4.17. [A.23] Manipulación de los equipos	3	4	5	4	ALTO
5.4.19. [A.25] Robo	4	4	5	5	MUY ALTO

- **HARDWARE- EQUIPOS INFORMÁTICOS: [HW_PC]**

Tabla F.26. Valoración del impacto potencial [HW_PC]

[HW] HARDWARE- EQUIPOS INFORMÁTICOS					
[HW_PC]	**Computadoras de escritorio**				
AMENAZAS	**IMPACTO POTENCIAL**				
	I: IMPACTO POTENCIAL POR DIMENSIONES			**IMPACTO TOTAL**	
	Ii	**Ic**	**Id**	**I-TOTAL**	**NIVEL**
5.1.1. [N.1] Fuego	1	2	4	3	MODERADO
5.1.2. [N.2] Daños por agua	3	2	4	3	MODERADO
5.2.3. [I.*] Desastres industriales	1	1	4	2	BAJO
5.2.6. [I.5] Avería de origen físico o lógico	2	2	4	3	MODERADO
5.2.7. [I.6] Corte del suministro eléctrico	3	4	4	4	ALTO
5.3.1. [E.1] Errores de los usuarios	4	4	4	4	ALTO
5.3.2. [E.2] Errores del administrador	4	4	4	4	ALTO
5.3.15. [E.23] Errores de mantenimiento / actualización de equipos (hardware)	3	4	4	4	ALTO
5.3.17. [E.25] Pérdida de equipos	4	4	4	4	ALTO
5.4.3. [A.5] Suplantación de la identidad del usuario	4	4	4	4	ALTO
5.4.4. [A.6] Abuso de privilegios de acceso	3	4	3	4	ALTO
5.4.9. [A.11] Acceso no autorizado	4	4	3	4	ALTO
5.4.17. [A.23] Manipulación de los equipos	4	4	3	4	ALTO
5.4.19. [A.25] Robo	1	2	4	3	MODERADO

- **HARDWARE- EQUIPOS INFORMÁTICOS: [HW_MV1]**

Tabla F.27. Valoración del impacto potencial [HW_MV1]

[HW] HARDWARE- EQUIPOS INFORMÁTICOS					
[HW_MV1]	**Computadoras Portátiles**				
AMENAZAS	**IMPACTO POTENCIAL**				
	I: IMPACTO POTENCIAL POR DIMENSIONES			**IMPACTO TOTAL**	
	Ii	**Ic**	**Id**	**I-TOTAL**	**NIVEL**
5.1.1. [N.1] Fuego	2	2	4	3	MODERADO
5.1.2. [N.2] Daños por agua	2	2	4	3	MODERADO
5.2.3. [I.*] Desastres industriales	1	2	4	3	MODERADO
5.2.6. [I.5] Avería de origen físico o lógico	2	4	4	4	ALTO
5.2.7. [I.6] Corte del suministro eléctrico	4	4	4	4	ALTO
5.3.1. [E.1] Errores de los usuarios	4	4	2	4	ALTO
5.3.2. [E.2] Errores del administrador	4	4	3	4	ALTO
5.3.15. [E.23] Errores de mantenimiento / actualización de equipos (hardware)	4	4	4	4	ALTO
5.3.17. [E.25] Pérdida de equipos	2	4	4	4	ALTO
5.4.3. [A.5] Suplantación de la identidad del usuario	4	4	4	4	ALTO
5.4.4. [A.6] Abuso de privilegios de acceso	4	4	3	4	ALTO
5.4.9. [A.11] Acceso no autorizado	3	4	3	4	ALTO
5.4.17. [A.23] Manipulación de los equipos	3	4	3	4	ALTO
5.4.19. [A.25] Robo	3	4	4	4	ALTO

- **HARDWARE- EQUIPOS INFORMÁTICOS: [HW_WAP]**

Tabla F.28. Valoración del impacto potencial [HW_WAP]

[HW] HARDWARE- EQUIPOS INFORMÁTICOS					
[HW_WAP]	**Punto de Acceso**				
AMENAZAS	**IMPACTO POTENCIAL**				
	I: IMPACTO POTENCIAL POR DIMENSIONES			**IMPACTO TOTAL**	
	Ii	**Ic**	**Id**	**I-TOTAL**	**NIVEL**
5.1.1. [N.1] Fuego	3	3	4	4	ALTO
5.1.2. [N.2] Daños por agua	3	3	4	4	ALTO
5.2.3. [I.*] Desastres industriales	3	3	4	4	ALTO
5.2.6. [I.5] Avería de origen físico o lógico	3	4	4	4	ALTO
5.2.7. [I.6] Corte del suministro eléctrico	4	4	4	4	ALTO
5.4.4. [A.6] Abuso de privilegios de acceso	3	4	3	4	ALTO
5.4.9. [A.11] Acceso no autorizado	4	4	3	4	ALTO
5.4.17. [A.23] Manipulación de los equipos	4	4	3	4	ALTO
5.4.19. [A.25] Robo	4	4	4	4	ALTO

- **HARDWARE- EQUIPOS INFORMÁTICOS: [HW_PT]**

Tabla F.29. Valoración del impacto potencial [HW_PT]

[HW] HARDWARE- EQUIPOS INFORMÁTICOS					
[HW_PT]	**Impresoras**				
AMENAZAS	**IMPACTO POTENCIAL**				
	I: IMPACTO POTENCIAL POR DIMENSIONES			**IMPACTO TOTAL**	
	Ii	**Ic**	**Id**	**I-TOTAL**	**NIVEL**
5.1.1. [N.1] Fuego	1	1	2	2	BAJO
5.1.2. [N.2] Daños por agua	1	1	2	2	BAJO
5.2.3. [I.*] Desastres industriales	1	1	2	2	BAJO
5.2.6. [I.5] Avería de origen físico o lógico	1	2	2	2	BAJO
5.2.7. [I.6] Corte del suministro eléctrico	2	2	2	2	BAJO
5.4.4. [A.6] Abuso de privilegios de acceso	1	2	2	2	BAJO
5.4.9. [A.11] Acceso no autorizado	2	2	2	2	BAJO
5.4.17. [A.23] Manipulación de los equipos	2	2	2	2	BAJO
5.4.19. [A.25] Robo	1	2	2	2	BAJO

- **REDES DE COMUNICACIONES: Internet Fibra Óptica**

Tabla F.30. Valoración del impacto potencial [Internet Fibra Óptica]

[COM] REDES DE COMUNICACIONES					
Internet Fibra Óptica	**Internet Fibra Óptica**				
AMENAZAS	**IMPACTO POTENCIAL**				
	I: IMPACTO POTENCIAL POR DIMENSIONES			**IMPACTO TOTAL**	
	Ii	**Ic**	**Id**	**I-TOTAL**	**NIVEL**
5.2.9. [I.8] Fallo de servicios de comunicaciones	2	4	5	4	ALTO
5.3.2. [E.2] Errores del administrador	3	5	5	5	MUY ALTO
5.3.11. [E.18] Destrucción de información	2	5	5	4	ALTO
5.3.12. [E.19] Fugas de información	2	5	5	4	ALTO
5.4.3. [A.5] Suplantación de la identidad del usuario	3	5	3	4	ALTO
5.4.4. [A.6] Abuso de privilegios de acceso	3	4	5	4	ALTO
5.4.9. [A.11] Acceso no autorizado	2	5	4	4	ALTO
5.4.10. [A.12] Análisis de tráfico	5	5	3	5	MUY ALTO
5.4.13. [A.15] Modificación deliberada de la información	4	3	3	4	ALTO
5.4.15. [A.19] Divulgación de información	2	3	3	3	MODERADO
5.4.18. [A.24] Denegación de servicio	2	4	5	4	ALTO

- **REDES DE COMUNICACIONES: [COM_LAN]**

Tabla F.31. Valoración del impacto potencial [COM_LAN]

[COM] REDES DE COMUNICACIONES					
[COM_LAN]	**Red Local**				
AMENAZAS	**IMPACTO POTENCIAL**				
	I: IMPACTO POTENCIAL POR DIMENSIONES			**IMPACTO TOTAL**	
	Ii	**Ic**	**Id**	**I-TOTAL**	**NIVEL**
5.2.9. [I.8] Fallo de servicios de comunicaciones	4	5	5	5	MUY ALTO
5.3.2. [E.2] Errores del administrador	5	5	5	5	MUY ALTO
5.3.11. [E.18] Destrucción de información	3	5	4	4	ALTO
5.3.12. [E.19] Fugas de información	5	5	5	5	MUY ALTO
5.4.3. [A.5] Suplantación de la identidad del usuario	3	5	3	4	ALTO
5.4.4. [A.6] Abuso de privilegios de acceso	4	4	5	5	MUY ALTO
5.4.9. [A.11] Acceso no autorizado	3	5	4	4	ALTO
5.4.10. [A.12] Análisis de tráfico	5	5	5	5	MUY ALTO
5.4.13. [A.15] Modificación deliberada de la información	5	5	5	5	MUY ALTO
5.4.15. [A.19] Divulgación de información	3	5	3	4	ALTO
5.4.18. [A.24] Denegación de servicio	3	4	5	4	ALTO

- **REDES DE COMUNICACIONES: [COM_MB]**

Tabla F.32. Valoración del impacto potencial [COM_MB]

[COM] REDES DE COMUNICACIONES					
[COM_MB]	**Telefonía Móvil**				
AMENAZAS	**IMPACTO POTENCIAL**				
	I: IMPACTO POTENCIAL POR DIMENSIONES			**IMPACTO TOTAL**	
	Ii	**Ic**	**Id**	**I-TOTAL**	**NIVEL**
5.2.9. [I.8] Fallo de servicios de comunicaciones	2	5	5	4	ALTO
5.3.2. [E.2] Errores del administrador	2	5	5	4	ALTO
5.3.11. [E.18] Destrucción de información	3	5	5	5	MUY ALTO
5.3.12. [E.19] Fugas de información	5	5	5	5	MUY ALTO
5.4.3. [A.5] Suplantación de la identidad del usuario	2	5	5	4	ALTO
5.4.4. [A.6] Abuso de privilegios de acceso	2	5	5	4	ALTO
5.4.9. [A.11] Acceso no autorizado	2	5	4	4	ALTO
5.4.10. [A.12] Análisis de tráfico	2	5	3	4	ALTO
5.4.13. [A.15] Modificación deliberada de la información	3	5	3	4	ALTO
5.4.15. [A.19] Divulgación de información	5	5	3	5	MUY ALTO
5.4.18. [A.24] Denegación de servicio	3	5	5	5	MUY ALTO

- **REDES DE COMUNICACIONES: [COM_WF]**

Tabla F.33. Valoración del impacto potencial [COM_WF]

[COM] REDES DE COMUNICACIONES					
[COM_WF]	**Red Inalámbrica**				
AMENAZAS	**IMPACTO POTENCIAL**				
	I: IMPACTO POTENCIAL POR DIMENSIONES			**IMPACTO TOTAL**	
	Ii	**Ic**	**Id**	**I-TOTAL**	**NIVEL**
5.2.9. [I.8] Fallo de servicios de comunicaciones	2	4	4	4	ALTO
5.3.2. [E.2] Errores del administrador	2	4	4	4	ALTO
5.3.11. [E.18] Destrucción de información	1	1	4	2	BAJO
5.3.12. [E.19] Fugas de información	4	4	3	4	ALTO
5.4.3. [A.5] Suplantación de la identidad del usuario	3	4	2	3	MODERADO
5.4.4. [A.6] Abuso de privilegios de acceso	3	4	3	4	ALTO
5.4.9. [A.11] Acceso no autorizado	3	4	4	4	ALTO
5.4.10. [A.12] Análisis de tráfico	3	4	3	4	ALTO
5.4.13. [A.15] Modificación deliberada de la información	4	3	2	3	MODERADO
5.4.15. [A.19] Divulgación de información	4	4	3	4	ALTO
5.4.18. [A.24] Denegación de servicio	3	4	4	4	ALTO

- **EQUIPO AUXILIAR: [AUX_CB]**

Tabla F.34. Valoración del impacto potencial [AUX_CB]

[AUX] EQUIPO AUXILIAR					
[AUX_CB]	**Cableado Estructurado**				
AMENAZAS	**IMPACTO POTENCIAL**				
	I: IMPACTO POTENCIAL POR DIMENSIONES			**IMPACTO TOTAL**	
	Ii	**Ic**	**Id**	**I-TOTAL**	**NIVEL**
5.1.1. [N.1] Fuego	2	2	5	3	MODERADO
5.1.2. [N.2] Daños por agua	2	3	5	4	ALTO
5.2.3. [I.*] Desastres industriales	2	2	5	3	MODERADO
5.2.4. [I.3] Contaminación mecánica	2	2	5	3	MODERADO
5.2.6. [I.5] Avería de origen físico o lógico	3	3	5	4	ALTO
5.2.7. [I.6] Corte del suministro eléctrico	3	2	5	4	ALTO
5.2.10. [I.9] Interrupción de otros servicios y suministros esenciales	2	3	5	4	ALTO
5.3.15. [E.23] Errores de mantenimiento / actualización de equipos (hardware)	4	5	5	5	MUY ALTO
5.3.17. [E.25] Pérdida de equipos	3	5	5	5	MUY ALTO
5.4.9. [A.11] Acceso no autorizado	2	5	3	4	ALTO
5.4.17. [A.23] Manipulación de los equipos	4	4	5	5	MUY ALTO
5.4.19. [A.25] Robo	3	5	5	5	MUY ALTO

- **EQUIPO AUXILIAR: [AUX_VIDEO]**

Tabla F.35. Valoración del impacto potencial [AUX_VIDEO]

[AUX] EQUIPO AUXILIAR					
[AUX_VIDEO]	**Sistema de Video vigilancia**				
AMENAZAS	**IMPACTO POTENCIAL**				
	I: IMPACTO POTENCIAL POR DIMENSIONES			**IMPACTO TOTAL**	
	Ii	**Ic**	**Id**	**I-TOTAL**	**NIVEL**
5.1.1. [N.1] Fuego	2	2	4	3	MODERADO
5.1.2. [N.2] Daños por agua	2	3	4	3	MODERADO
5.2.3. [I.*] Desastres industriales	2	2	4	3	MODERADO
5.2.4. [I.3] Contaminación mecánica	2	2	4	3	MODERADO
5.2.6. [I.5] Avería de origen físico o lógico	2	3	4	3	MODERADO
5.2.7. [I.6] Corte del suministro eléctrico	4	4	4	4	ALTO
5.2.10. [I.9] Interrupción de otros servicios y suministros esenciales	3	3	4	4	ALTO
5.3.15. [E.23] Errores de mantenimiento / actualización de equipos (hardware)	3	4	4	4	ALTO
5.3.17. [E.25] Pérdida de equipos	1	3	4	3	MODERADO
5.4.9. [A.11] Acceso no autorizado	2	4	4	4	ALTO
5.4.17. [A.23] Manipulación de los equipos	4	4	4	4	ALTO
5.4.19. [A.25] Robo	1	3	4	3	MODERADO

- **EQUIPO AUXILIAR: [AUX_UPS]**

Tabla F.36. Valoración del impacto potencial [AUX_UPS]

[AUX] EQUIPO AUXILIAR					
[AUX_UPS]	**Sistema de alimentación Interrumpida**				
AMENAZAS	**IMPACTO POTENCIAL**				
	I: IMPACTO POTENCIAL POR DIMENSIONES			**IMPACTO TOTAL**	
	Ii	**Ic**	**Id**	**I-TOTAL**	**NIVEL**
5.1.1. [N.1] Fuego	1	2	3	2	BAJO
5.1.2. [N.2] Daños por agua	1	2	3	2	BAJO
5.2.3. [I.*] Desastres industriales	1	2	3	2	BAJO
5.2.4. [I.3] Contaminación mecánica	2	2	3	3	MODERADO
5.2.6. [I.5] Avería de origen físico o lógico	2	2	3	3	MODERADO
5.2.7. [I.6] Corte del suministro eléctrico	3	3	3	3	MODERADO
5.3.15. [E.23] Errores de mantenimiento / actualización de equipos (hardware)	1	2	3	2	BAJO
5.3.17. [E.25] Pérdida de equipos	2	2	3	3	MODERADO
5.4.17. [A.23] Manipulación de los equipos	2	1	3	2	BAJO
5.4.19. [A.25] Robo	2	2	3	3	MODERADO

G. ANEXO G: VALORACIÓN DEL RIESGO POTENCIAL

- **INFORMACIÓN: [INFO_VR]**

Tabla G.1. Valoración del Riesgo Potencial [INFO_VR]

[INFO] INFORMACIÓN					
[INFO_VR]	**Registros confidenciales de la organización**				
AMENAZAS	**RIESGO POTENCIAL**				
	RIESGO POTENCIAL POR DIMENSIONES			**RIESGO POTENCIAL TOTAL**	
	Ri	**Rc**	**Rd**	**Rt**	**NIVEL**
5.3.1. [E.1] Errores de los usuarios	5	5	5	5	MUY ALTO
5.3.2. [E.2] Errores del administrador	5	5	5	5	MUY ALTO
5.3.10. [E.15] Alteración accidental de la información	4	1	1	2	BAJO
5.3.11. [E.18] Destrucción de información	2	2	2	2	BAJO
5.3.12. [E.19] Fugas de información	1	2	1	2	BAJO
5.4.3. [A.5] Suplantación de la identidad del usuario	3	3	1	3	MODERADO
5.4.4. [A.6] Abuso de privilegios de acceso	3	3	3	3	MODERADO
5.4.9. [A.11] Acceso no autorizado	3	3	1	3	MODERADO
5.4.13. [A.15] Modificación deliberada de la información	3	2	2	3	MODERADO
5.4.15. [A.19] Divulgación de información	4	4	1	3	MODERADO

- **INFORMACIÓN: [INFO_PER]**

Tabla G.2. Valoración del Riesgo Potencial [INFO_PER]

[INFO] INFORMACIÓN					
[INFO_PER]	**Base de datos de clientes y proveedores**				
AMENAZAS	**RIESGO POTENCIAL**				
	RIESGO POTENCIAL POR DIMENSIONES			**RIESGO POTENCIAL TOTAL**	
	Ri	**Rc**	**Rd**	**Rt**	**NIVEL**
5.3.1. [E.1] Errores de los usuarios	4	4	4	4	ALTO
5.3.2. [E.2] Errores del administrador	5	5	5	5	MUY ALTO
5.3.10. [E.15] Alteración accidental de la información	3	3	3	3	MODERADO
5.3.11. [E.18] Destrucción de información	2	3	3	3	MODERADO
5.3.12. [E.19] Fugas de información	4	4	4	4	ALTO
5.4.3. [A.5] Suplantación de la identidad del usuario	3	3	1	3	MODERADO
5.4.4. [A.6] Abuso de privilegios de acceso	2	2	2	2	BAJO
5.4.9. [A.11] Acceso no autorizado	3	3	2	3	MODERADO
5.4.13. [A.15] Modificación deliberada de la información	2	2	1	2	BAJO
5.4.15. [A.19] Divulgación de información	4	4	1	3	MODERADO

- **INFORMACIÓN: [INFO_PUB]**

Tabla G.3. Valoración del Riesgo Potencial [INFO_PUB]

[INFO] INFORMACIÓN					
[INFO_PUB]	**Documentación y permisos de funcionamiento**				
AMENAZAS	**RIESGO POTENCIAL**				
	RIESGO POTENCIAL POR DIMENSIONES			**RIESGO POTENCIAL TOTAL**	
	Ri	**Rc**	**Rd**	**Rt**	**NIVEL**
5.3.1. [E.1] Errores de los usuarios	4	4	5	5	MUY ALTO
5.3.2. [E.2] Errores del administrador	5	5	5	5	MUY ALTO
5.3.10. [E.15] Alteración accidental de la información	4	1	4	3	MODERADO
5.3.11. [E.18] Destrucción de información	2	2	2	2	BAJO
5.3.12. [E.19] Fugas de información	1	2	2	2	BAJO
5.4.3. [A.5] Suplantación de la identidad del usuario	2	2	1	2	BAJO
5.4.4. [A.6] Abuso de privilegios de acceso	2	2	1	2	BAJO
5.4.9. [A.11] Acceso no autorizado	2	2	2	2	BAJO
5.4.13. [A.15] Modificación deliberada de la información	3	2	2	3	MODERADO
5.4.15. [A.19] Divulgación de información	4	4	4	4	ALTO

- **DATOS E INFORMACIÓN COMPLEMENTARIA: [D_BCK]**

Tabla G.4. Valoración del Riesgo Potencial [D_BCK]

[D] DATOS E INFORMACIÓN COMPLEMENTARIA					
[D_BCK]	**Copias de seguridad OwnCloud**				
AMENAZAS	**RIESGO POTENCIAL**				
	RIESGO POTENCIAL POR DIMENSIONES			**RIESGO POTENCIAL TOTAL**	
	Ri	**Rc**	**Rd**	**Rt**	**NIVEL**
5.3.1. [E.1] Errores de los usuarios	2	2	2	2	BAJO
5.3.2. [E.2] Errores del administrador	4	4	4	4	ALTO
5.3.10. [E.15] Alteración accidental de la información	3	3	2	3	MODERADO
5.3.11. [E.18] Destrucción de información	1	2	2	2	BAJO
5.3.12. [E.19] Fugas de información	2	2	1	2	BAJO
5.4.3. [A.5] Suplantación de la identidad del usuario	3	3	2	3	MODERADO
5.4.4. [A.6] Abuso de privilegios de acceso	3	3	3	3	MODERADO
5.4.9. [A.11] Acceso no autorizado	3	3	3	3	MODERADO
5.4.13. [A.15] Modificación deliberada de la información	3	2	2	3	MODERADO
5.4.15. [A.19] Divulgación de información	3	4	4	4	ALTO

- **DATOS E INFORMACIÓN COMPLEMENTARIA: [D_LG]**

Tabla G.5. Valoración del Riesgo Potencial [D_LG]

[D] DATOS E INFORMACIÓN COMPLEMENTARIA					
[D_LG]	**Logs de SACI**				
AMENAZAS	**RIESGO POTENCIAL**				
	RIESGO POTENCIAL POR DIMENSIONES			**RIESGO POTENCIAL TOTAL**	
	Ri	**Rc**	**Rd**	**Rt**	**NIVEL**
5.3.1. [E.1] Errores de los usuarios	3	3	3	3	MODERADO
5.3.2. [E.2] Errores del administrador	4	4	4	4	ALTO
5.3.3. [E.3] Errores de monitorización (log)	4	4	2	4	ALTO
5.3.10. [E.15] Alteración accidental de la información	3	3	2	3	MODERADO
5.3.11. [E.18] Destrucción de información	1	2	2	2	BAJO
5.3.12. [E.19] Fugas de información	4	4	3	4	ALTO
5.4.1. [A.3] Manipulación de los registros de actividad (log)	2	2	2	2	BAJO
5.4.3. [A.5] Suplantación de la identidad del usuario	3	3	2	3	MODERADO
5.4.4. [A.6] Abuso de privilegios de acceso	3	3	3	3	MODERADO
5.4.9. [A.11] Acceso no autorizado	2	2	1	2	BAJO
5.4.13. [A.15] Modificación deliberada de la información	3	2	2	3	MODERADO
5.4.15. [A.19] Divulgación de información	3	4	3	4	ALTO

- **CLAVES CRIPTOGRÁFICAS: [K_PB]**

Tabla G.6. Valoración del Riesgo Potencial [K_PB]

[K] CLAVES CRIPTOGRÁFICAS					
[K_PB]	**SSL**				
AMENAZAS	**RIESGO POTENCIAL**				
	RIESGO POTENCIAL POR DIMENSIONES			**RIESGO POTENCIAL TOTAL**	
	Ri	**Rc**	**Rd**	**Rt**	**NIVEL**
5.3.1. [E.1] Errores de los usuarios	2	2	2	2	BAJO
5.3.2. [E.2] Errores del administrador	4	4	4	4	ALTO
5.3.10. [E.15] Alteración accidental de la información	3	2	1	2	BAJO
5.3.11. [E.18] Destrucción de información	1	1	2	2	BAJO
5.3.12. [E.19] Fugas de información	1	3	2	2	BAJO
5.4.3. [A.5] Suplantación de la identidad del usuario	2	2	2	2	BAJO
5.4.4. [A.6] Abuso de privilegios de acceso	2	2	2	2	BAJO
5.4.9. [A.11] Acceso no autorizado	3	3	3	3	MODERADO
5.4.13. [A.15] Modificación deliberada de la información	2	2	2	2	BAJO
5.4.15. [A.19] Divulgación de información	1	2	1	2	BAJO

- **CLAVES CRIPTOGRÁFICAS: [K_SIGN]**

Tabla G.7. Valoración del Riesgo Potencial [K_SIGN]

[K] CLAVES CRIPTOGRÁFICAS					
[K_SIGN]	**Token Digital**				
AMENAZAS	**RIESGO POTENCIAL**				
	RIESGO POTENCIAL POR DIMENSIONES			**RIESGO POTENCIAL TOTAL**	
	Ri	**Rc**	**Rd**	**Rt**	**NIVEL**
5.3.1. [E.1] Errores de los usuarios	2	3	2	3	MODERADO
5.3.2. [E.2] Errores del administrador	4	4	4	4	ALTO
5.3.10. [E.15] Alteración accidental de la información	4	4	4	4	ALTO
5.3.11. [E.18] Destrucción de información	2	2	2	2	BAJO
5.3.12. [E.19] Fugas de información	2	2	2	2	BAJO
5.4.3. [A.5] Suplantación de la identidad del usuario	3	3	3	3	MODERADO
5.4.4. [A.6] Abuso de privilegios de acceso	2	2	2	2	BAJO
5.4.9. [A.11] Acceso no autorizado	3	3	2	3	MODERADO
5.4.13. [A.15] Modificación deliberada de la información	2	2	2	2	BAJO
5.4.15. [A.19] Divulgación de información	2	2	2	2	BAJO

- **SERVICIOS: [S_INT]**

Tabla G.8. Valoración del Riesgo Potencial [S_INT]

[S] SERVICIOS					
[S_INT]	**Servicio del sistema contable**				
AMENAZAS	**RIESGO POTENCIAL**				
	RIESGO POTENCIAL POR DIMENSIONES			**RIESGO POTENCIAL TOTAL**	
	Ri	**Rc**	**Rd**	**Rt**	**NIVEL**
5.3.1. [E.1] Errores de los usuarios	5	5	4	5	MUY ALTO
5.3.2. [E.2] Errores del administrador	5	5	5	5	MUY ALTO
5.3.10. [E.15] Alteración accidental de la información	4	3	1	3	MODERADO
5.3.11. [E.18] Destrucción de información	1	2	2	2	BAJO
5.3.12. [E.19] Fugas de información	1	4	2	3	MODERADO
5.4.3. [A.5] Suplantación de la identidad del usuario	4	4	3	4	ALTO
5.4.4. [A.6] Abuso de privilegios de acceso	2	2	2	2	BAJO
5.4.9. [A.11] Acceso no autorizado	3	3	1	3	MODERADO
5.4.13. [A.15] Modificación deliberada de la información	2	2	1	2	BAJO
5.4.15. [A.19] Divulgación de información	2	4	2	3	MODERADO

- **SERVICIOS: [S_WWW]**

Tabla G.9. Valoración del Riesgo Potencial [S_WWW]

[S] SERVICIOS					
[S_WWW]	**Sitio web**				
AMENAZAS	**RIESGO POTENCIAL**				
	RIESGO POTENCIAL POR DIMENSIONES			**RIESGO POTENCIAL TOTAL**	
	Ri	**Rc**	**Rd**	**Rt**	**NIVEL**
5.3.1. [E.1] Errores de los usuarios	4	4	4	4	ALTO
5.3.2. [E.2] Errores del administrador	4	4	4	4	ALTO
5.3.10. [E.15] Alteración accidental de la información	4	4	3	4	ALTO
5.3.11. [E.18] Destrucción de información	1	2	2	2	BAJO
5.3.12. [E.19] Fugas de información	2	4	4	4	ALTO
5.4.3. [A.5] Suplantación de la identidad del usuario	4	4	4	4	ALTO
5.4.4. [A.6] Abuso de privilegios de acceso	2	2	2	2	BAJO
5.4.9. [A.11] Acceso no autorizado	3	3	2	3	MODERADO
5.4.13. [A.15] Modificación deliberada de la información	2	2	1	2	BAJO
5.4.15. [A.19] Divulgación de información	2	4	1	3	MODERADO
5.4.18. [A.24] Denegación de servicio	1	2	2	2	BAJO

- **SOFTWARE- APLICACIONES INFORMÁTICAS: [SW_HP]**

Tabla G.10. Valoración del Riesgo Potencial [SW_HP]

[SW] SOFTWARE- APLICACIONES INFORMÁTICAS					
[SW_HP]	**Proxmox**				
AMENAZAS	**RIESGO POTENCIAL**				
	RIESGO POTENCIAL POR DIMENSIONES			**RIESGO POTENCIAL TOTAL**	
	Ri	**Rc**	**Rd**	**Rt**	**NIVEL**
5.2.6. [I.5] Avería de origen físico o lógico	1	4	5	4	ALTO
5.3.1. [E.1] Errores de los usuarios	3	3	3	3	MODERADO
5.3.2. [E.2] Errores del administrador	2	2	2	2	BAJO
5.3.6. [E.8] Difusión de software dañino	3	3	3	3	MODERADO
5.3.10. [E.15] Alteración accidental de la información	2	2	2	2	BAJO
5.3.11. [E.18] Destrucción de información	2	2	2	2	BAJO
5.3.12. [E.19] Fugas de información	2	3	3	3	MODERADO
5.3.13. [E.20] Vulnerabilidades de los programas (software)	5	5	5	5	MUY ALTO
5.3.14. [E.21] Errores de mantenimiento / actualización de programas (software)	5	3	5	5	MUY ALTO
5.4.3. [A.5] Suplantación de la identidad del usuario	2	2	2	2	BAJO
5.4.4. [A.6] Abuso de privilegios de acceso	4	4	4	4	ALTO
5.4.9. [A.11] Acceso no autorizado	3	3	2	3	MODERADO
5.4.13. [A.15] Modificación deliberada de la información	3	3	2	3	MODERADO
5.4.15. [A.19] Divulgación de información	1	3	2	2	BAJO
5.4.16. [A.22] Manipulación de programas	4	4	4	4	ALTO
5.4.18. [A.24] Denegación de servicio	1	2	2	2	BAJO

- **SOFTWARE- APLICACIONES INFORMÁTICAS: [SW_BD1]**

Tabla G.11. Valoración del Riesgo Potencial [SW_BD1]

[SW] SOFTWARE- APLICACIONES INFORMÁTICAS					
[SW_BD1]	**Servidor de Base de Datos Oracle XE 18c**				
AMENAZAS	**RIESGO POTENCIAL**				
	RIESGO POTENCIAL POR DIMENSIONES			**RIESGO POTENCIAL TOTAL**	
	Ri	**Rc**	**Rd**	**Rt**	**NIVEL**
5.2.6. [I.5] Avería de origen físico o lógico	2	2	2	2	BAJO
5.3.1. [E.1] Errores de los usuarios	4	4	4	4	ALTO
5.3.2. [E.2] Errores del administrador	4	4	4	4	ALTO
5.3.6. [E.8] Difusión de software dañino	3	3	3	3	MODERADO
5.3.10. [E.15] Alteración accidental de la información	2	2	2	2	BAJO
5.3.11. [E.18] Destrucción de información	1	2	2	2	BAJO
5.3.12. [E.19] Fugas de información	2	3	2	3	MODERADO
5.4.3. [A.5] Suplantación de la identidad del usuario	2	2	2	2	BAJO
5.4.9. [A.11] Acceso no autorizado	2	2	1	2	BAJO
5.4.13. [A.15] Modificación deliberada de la información	3	3	2	3	MODERADO
5.4.15. [A.19] Divulgación de información	2	4	2	3	MODERADO
5.4.18. [A.24] Denegación de servicio	1	2	2	2	BAJO

- **SOFTWARE- APLICACIONES INFORMÁTICAS: [SW_APP4]**

Tabla G.12. Valoración del Riesgo Potencial [SW_APP4]

[SW] SOFTWARE- APLICACIONES INFORMÁTICAS					
[SW_APP4]	**Servidor Digital Ocean**				
AMENAZAS	**RIESGO POTENCIAL**				
	RIESGO POTENCIAL POR DIMENSIONES			**RIESGO POTENCIAL TOTAL**	
	Ri	**Rc**	**Rd**	**Rt**	**NIVEL**
5.2.6. [I.5] Avería de origen físico o lógico	2	3	3	3	MODERADO
5.3.2. [E.2] Errores del administrador	3	4	4	4	ALTO
5.3.6. [E.8] Difusión de software dañino	2	3	3	3	MODERADO
5.4.3. [A.5] Suplantación de la identidad del usuario	2	2	2	2	BAJO
5.4.4. [A.6] Abuso de privilegios de acceso	3	4	4	4	ALTO
5.4.9. [A.11] Acceso no autorizado	2	3	2	3	MODERADO

- **SOFTWARE- APLICACIONES INFORMÁTICAS: [SW_APP2]**

Tabla G.13. Valoración del Riesgo Potencial [SW_APP2]

[SW] SOFTWARE- APLICACIONES INFORMÁTICAS					
[SW_APP2]	**Servidor FTP**				
AMENAZAS	**RIESGO POTENCIAL**				
	RIESGO POTENCIAL POR DIMENSIONES			**RIESGO POTENCIAL TOTAL**	
	Ri	**Rc**	**Rd**	**Rt**	**NIVEL**
5.2.6. [I.5] Avería de origen físico o lógico	3	3	3	3	MODERADO
5.3.2. [E.2] Errores del administrador	3	3	1	3	MODERADO
5.3.6. [E.8] Difusión de software dañino	2	3	3	3	MODERADO
5.3.10. [E.15] Alteración accidental de la información	2	2	1	2	BAJO
5.3.11. [E.18] Destrucción de información	1	1	1	1	MUY BAJO
5.4.3. [A.5] Suplantación de la identidad del usuario	2	2	1	2	BAJO
5.4.4. [A.6] Abuso de privilegios de acceso	4	4	4	4	ALTO
5.4.9. [A.11] Acceso no autorizado	3	3	2	3	MODERADO
5.4.18. [A.24] Denegación de servicio	1	1	1	1	MUY BAJO

- **SOFTWARE- APLICACIONES INFORMÁTICAS: [SW_BD2]**

Tabla G.14. Valoración del Riesgo Potencial [SW_BD2]

[SW] SOFTWARE- APLICACIONES INFORMÁTICAS					
[SW_BD2]	**Servidor de Base de Datos MySQL 8.0**				
AMENAZAS	**RIESGO POTENCIAL**				
	RIESGO POTENCIAL POR DIMENSIONES			**RIESGO POTENCIAL TOTAL**	
	Ri	**Rc**	**Rd**	**Rt**	**NIVEL**
5.2.6. [I.5] Avería de origen físico o lógico	3	3	3	3	MODERADO
5.3.1. [E.1] Errores de los usuarios	4	4	3	4	ALTO
5.3.2. [E.2] Errores del administrador	4	4	4	4	ALTO
5.3.6. [E.8] Difusión de software dañino	2	3	3	3	MODERADO
5.3.10. [E.15] Alteración accidental de la información	2	2	2	2	BAJO
5.3.11. [E.18] Destrucción de información	1	1	1	1	MUY BAJO
5.3.12. [E.19] Fugas de información	1	3	2	2	BAJO
5.4.3. [A.5] Suplantación de la identidad del usuario	1	2	2	2	BAJO
5.4.9. [A.11] Acceso no autorizado	4	4	2	4	ALTO
5.4.13. [A.15] Modificación deliberada de la información	3	3	2	3	MODERADO
5.4.15. [A.19] Divulgación de información	1	4	2	3	MODERADO
5.4.18. [A.24] Denegación de servicio	1	2	2	3	MODERADO

- **SOFTWARE- APLICACIONES INFORMÁTICAS: [SW_APP3]**

Tabla G.15. Valoración del Riesgo Potencial [SW_APP3]

[SW] SOFTWARE- APLICACIONES INFORMÁTICAS					
[SW_APP3]	**Servidor DNS**				
AMENAZAS	**RIESGO POTENCIAL**				
	RIESGO POTENCIAL POR DIMENSIONES			**RIESGO POTENCIAL TOTAL**	
	Ri	**Rc**	**Rd**	**Rt**	**NIVEL**
5.2.6. [I.5] Avería de origen físico o lógico	2	3	3	3	MODERADO
5.3.2. [E.2] Errores del administrador	4	4	4	4	ALTO
5.3.6. [E.8] Difusión de software dañino	1	3	3	3	MODERADO
5.4.3. [A.5] Suplantación de la identidad del usuario	2	2	2	2	BAJO
5.4.4. [A.6] Abuso de privilegios de acceso	4	4	4	4	ALTO
5.4.9. [A.11] Acceso no autorizado	3	3	2	3	MODERADO
5.4.18. [A.24] Denegación de servicio	1	2	2	2	BAJO

- **SOFTWARE- APLICACIONES INFORMÁTICAS: [SW_BD3]**

Tabla G.16. Valoración del Riesgo Potencial [SW_BD3]

[SW] SOFTWARE- APLICACIONES INFORMÁTICAS					
[SW_BD3]	**Servidor de Base de Datos Postgresql 13**				
AMENAZAS	**RIESGO POTENCIAL**				
	RIESGO POTENCIAL POR DIMENSIONES			**RIESGO POTENCIAL TOTAL**	
	Ri	**Rc**	**Rd**	**Rt**	**NIVEL**
5.2.6. [I.5] Avería de origen físico o lógico	1	3	3	3	MODERADO
5.3.1. [E.1] Errores de los usuarios	4	4	4	4	ALTO
5.3.2. [E.2] Errores del administrador	4	4	4	4	ALTO
5.3.6. [E.8] Difusión de software dañino	3	2	3	3	MODERADO
5.3.10. [E.15] Alteración accidental de la información	4	4	3	4	ALTO
5.3.11. [E.18] Destrucción de información	1	2	2	2	BAJO
5.3.12. [E.19] Fugas de información	2	4	3	3	MODERADO
5.4.3. [A.5] Suplantación de la identidad del usuario	1	2	1	2	BAJO
5.4.9. [A.11] Acceso no autorizado	2	3	2	3	MODERADO
5.4.13. [A.15] Modificación deliberada de la información	3	3	2	3	MODERADO
5.4.15. [A.19] Divulgación de información	1	4	2	3	MODERADO
5.4.18. [A.24] Denegación de servicio	1	2	2	2	BAJO

- **SOFTWARE- APLICACIONES INFORMÁTICAS: [SW_AV]**

Tabla G.17. Valoración del Riesgo Potencial [SW_AV]

[SW] SOFTWARE- APLICACIONES INFORMÁTICAS					
[SW_AV]	**Avast Free Antivirus**				
AMENAZAS	**RIESGO POTENCIAL**				
	RIESGO POTENCIAL POR DIMENSIONES			**RIESGO POTENCIAL TOTAL**	
	Ri	**Rc**	**Rd**	**Rt**	**NIVEL**
5.2.6. [I.5] Avería de origen físico o lógico	2	3	3	3	MODERADO
5.3.1. [E.1] Errores de los usuarios	3	4	4	4	ALTO
5.3.2. [E.2] Errores del administrador	3	4	4	4	ALTO
5.3.6. [E.8] Difusión de software dañino	4	4	4	4	ALTO
5.3.13. [E.20] Vulnerabilidades de los programas (software)	2	5	5	4	ALTO
5.3.14. [E.21] Errores de mantenimiento / actualización de programas (software)	2	5	5	4	ALTO
5.4.3. [A.5] Suplantación de la identidad del usuario	3	3	3	3	MODERADO
5.4.4. [A.6] Abuso de privilegios de acceso	4	4	4	4	ALTO
5.4.9. [A.11] Acceso no autorizado	2	3	2	3	MODERADO

- **SOFTWARE- APLICACIONES INFORMÁTICAS: [SW_APP1]**

Tabla G.18. Valoración del Riesgo Potencial [SW_APP1]

[SW] SOFTWARE- APLICACIONES INFORMÁTICAS					
[SW_APP1]	**Servidor de OwnCloud**				
AMENAZAS	**RIESGO POTENCIAL**				
	RIESGO POTENCIAL POR DIMENSIONES			**RIESGO POTENCIAL TOTAL**	
	Ri	**Rc**	**Rd**	**Rt**	**NIVEL**
5.2.6. [I.5] Avería de origen físico o lógico	3	3	3	3	MODERADO
5.3.1. [E.1] Errores de los usuarios	4	4	2	4	ALTO
5.3.2. [E.2] Errores del administrador	4	4	4	4	ALTO
5.3.6. [E.8] Difusión de software dañino	3	3	3	3	MODERADO
5.3.10. [E.15] Alteración accidental de la información	3	3	3	3	MODERADO
5.3.11. [E.18] Destrucción de información	1	1	1	1	MUY BAJO
5.3.12. [E.19] Fugas de información	2	4	3	3	MODERADO
5.3.14. [E.21] Errores de mantenimiento / actualización de programas (software)	2	4	4	4	ALTO
5.4.3. [A.5] Suplantación de la identidad del usuario	3	3	2	3	MODERADO
5.4.4. [A.6] Abuso de privilegios de acceso	4	4	4	4	ALTO
5.4.9. [A.11] Acceso no autorizado	3	3	2	3	MODERADO
5.4.13. [A.15] Modificación deliberada de la información	3	3	2	3	MODERADO
5.4.15. [A.19] Divulgación de información	1	4	1	2	BAJO
5.4.18. [A.24] Denegación de servicio	1	1	1	1	MUY BAJO

- **SOFTWARE- APLICACIONES INFORMÁTICAS: [SW_WWW]**

Tabla G.19. Valoración del Riesgo Potencial [SW_WWW]

[SW] SOFTWARE- APLICACIONES INFORMÁTICAS					
[SW_WWW]	**Servidor Web NGINX**				
AMENAZAS	**RIESGO POTENCIAL**				
	RIESGO POTENCIAL POR DIMENSIONES			**RIESGO POTENCIAL TOTAL**	
	Ri	**Rc**	**Rd**	**Rt**	**NIVEL**
5.2.6. [I.5] Avería de origen físico o lógico	2	2	2	2	BAJO
5.3.2. [E.2] Errores del administrador	2	3	3	3	MODERADO
5.3.6. [E.8] Difusión de software dañino	2	2	2	2	BAJO
5.4.3. [A.5] Suplantación de la identidad del usuario	1	1	1	1	MUY BAJO
5.4.4. [A.6] Abuso de privilegios de acceso	3	3	3	3	MODERADO
5.4.9. [A.11] Acceso no autorizado	2	2	2	2	BAJO
5.4.18. [A.24] Denegación de servicio	1	1	1	1	MUY BAJO

- **SOFTWARE- APLICACIONES INFORMÁTICAS: [SW_OS]**

Tabla G.20. Valoración del Riesgo Potencial [SW_OS]

[SW] SOFTWARE- APLICACIONES INFORMÁTICAS					
[SW_OS]	**Windows/Linux**				
AMENAZAS	**RIESGO POTENCIAL**				
	RIESGO POTENCIAL POR DIMENSIONES			**RIESGO POTENCIAL TOTAL**	
	Ri	**Rc**	**Rd**	**Rt**	**NIVEL**
5.2.6. [I.5] Avería de origen físico o lógico	1	3	4	3	MODERADO
5.3.1. [E.1] Errores de los usuarios	4	4	4	4	ALTO
5.3.2. [E.2] Errores del administrador	4	4	4	4	ALTO
5.3.6. [E.8] Difusión de software dañino	2	2	3	3	MODERADO
5.3.10. [E.15] Alteración accidental de la información	1	2	2	2	BAJO
5.3.11. [E.18] Destrucción de información	1	1	1	1	MUY BAJO
5.3.12. [E.19] Fugas de información	2	4	3	3	MODERADO
5.3.13. [E.20] Vulnerabilidades de los programas (software)	4	4	4	4	ALTO
5.3.14. [E.21] Errores de mantenimiento / actualización de programas (software)	4	4	4	4	ALTO
5.4.3. [A.5] Suplantación de la identidad del usuario	1	2	2	2	BAJO
5.4.4. [A.6] Abuso de privilegios de acceso	1	4	4	3	MODERADO
5.4.9. [A.11] Acceso no autorizado	2	3	2	3	MODERADO
5.4.13. [A.15] Modificación deliberada de la información	3	3	2	3	MODERADO
5.4.15. [A.19] Divulgación de información	1	4	2	3	MODERADO
5.4.18. [A.24] Denegación de servicio	1	2	2	2	BAJO

- **SOFTWARE- APLICACIONES INFORMÁTICAS: [SW_ALM]**

Tabla G.21. Valoración del riesgo potencial [SW_ALM]

[SW] SOFTWARE- APLICACIONES INFORMÁTICAS					
[SW_ALM]	**Google Drive**				
AMENAZAS	**RIESGO POTENCIAL**				
	RIESGO POTENCIAL POR DIMENSIONES			**RIESGO POTENCIAL TOTAL**	
	Ri	**Rc**	**Rd**	**Rt**	**NIVEL**
5.3.1. [E.1] Errores de los usuarios	2	3	3	3	MODERADO
5.3.2. [E.2] Errores del administrador	3	3	3	3	MODERADO
5.3.10. [E.15] Alteración accidental de la información	2	2	2	2	BAJO
5.3.11. [E.18] Destrucción de información	1	1	1	1	MUY BAJO
5.3.12. [E.19] Fugas de información	3	3	3	3	MODERADO
5.4.3. [A.5] Suplantación de la identidad del usuario	2	2	2	2	BAJO
5.4.4. [A.6] Abuso de privilegios de acceso	3	3	2	3	MODERADO
5.4.9. [A.11] Acceso no autorizado	2	2	2	2	BAJO
5.4.13. [A.15] Modificación deliberada de la información	2	2	2	2	BAJO
5.4.15. [A.19] Divulgación de información	2	3	2	3	MODERADO
5.4.18. [A.24] Denegación de servicio	1	2	2	2	BAJO

- **SOFTWARE- APLICACIONES INFORMÁTICAS: [SW_OFF]**

Tabla G.22. Valoración del Riesgo Potencial [SW_OFF]

[SW] SOFTWARE- APLICACIONES INFORMÁTICAS					
[SW_OFF]	**Microsoft Office Professional 2019**				
AMENAZAS	**RIESGO POTENCIAL**				
	RIESGO POTENCIAL POR DIMENSIONES			**RIESGO POTENCIAL TOTAL**	
	Ri	**Rc**	**Rd**	**Rt**	**NIVEL**
5.2.6. [I.5] Avería de origen físico o lógico	1	3	3	3	MODERADO
5.3.1. [E.1] Errores de los usuarios	2	2	2	2	BAJO
5.3.2. [E.2] Errores del administrador	2	2	2	2	BAJO
5.3.6. [E.8] Difusión de software dañino	2	2	2	2	BAJO
5.3.14. [E.21] Errores de mantenimiento / actualización de programas (software)	2	2	2	2	BAJO
5.4.3. [A.5] Suplantación de la identidad del usuario	1	2	2	2	BAJO
5.4.4. [A.6] Abuso de privilegios de acceso	3	3	2	3	MODERADO
5.4.9. [A.11] Acceso no autorizado	2	2	2	2	BAJO
5.4.18. [A.24] Denegación de servicio	1	2	2	2	BAJO

- **HARDWARE- EQUIPOS INFORMÁTICOS: [HW_HT]**

Tabla G.23. Valoración del Riesgo Potencial [HW_HT]

[HW] HARDWARE- EQUIPOS INFORMÁTICOS					
[HW_HT]	**Servidor físico HP Proliant DL 360P**				
AMENAZAS	**RIESGO POTENCIAL**				
	RIESGO POTENCIAL POR DIMENSIONES			**RIESGO POTENCIAL TOTAL**	
	Ri	**Rc**	**Rd**	**Rt**	**NIVEL**
5.1.1. [N.1] Fuego	2	3	3	3	MODERADO
5.1.2. [N.2] Daños por agua	2	3	3	3	MODERADO
5.2.3. [I.*] Desastres industriales	2	2	2	2	BAJO
5.2.6. [I.5] Avería de origen físico o lógico	2	3	3	3	MODERADO
5.2.7. [I.6] Corte del suministro eléctrico	4	4	5	5	MUY ALTO
5.3.2. [E.2] Errores del administrador	4	4	4	4	ALTO
5.3.15. [E.23] Errores de mantenimiento / actualización de equipos (hardware)	3	3	3	3	MODERADO
5.3.17. [E.25] Pérdida de equipos	2	2	2	2	BAJO
5.4.4. [A.6] Abuso de privilegios de acceso	2	2	2	2	BAJO
5.4.9. [A.11] Acceso no autorizado	3	3	2	3	MODERADO
5.4.17. [A.23] Manipulación de los equipos	2	2	2	2	BAJO
5.4.19. [A.25] Robo	2	2	2	2	BAJO

- **HARDWARE- EQUIPOS INFORMÁTICOS: [HW_SW]**

Tabla G.24. Valoración del Riesgo Potencial [HW_SW]

[HW] HARDWARE- EQUIPOS INFORMÁTICOS					
[HW_SW]	**Switch TP-LINK**				
AMENAZAS	**RIESGO POTENCIAL**				
	RIESGO POTENCIAL POR DIMENSIONES			**RIESGO POTENCIAL TOTAL**	
	Ri	**Rc**	**Rd**	**Rt**	**NIVEL**
5.1.1. [N.1] Fuego	2	3	3	3	MODERADO
5.1.2. [N.2] Daños por agua	2	2	3	3	MODERADO
5.2.3. [I.*] Desastres industriales	2	2	2	2	BAJO
5.2.6. [I.5] Avería de origen físico o lógico	3	2	3	3	MODERADO
5.2.7. [I.6] Corte del suministro eléctrico	4	5	5	5	MUY ALTO
5.3.2. [E.2] Errores del administrador	3	4	4	4	ALTO
5.3.15. [E.23] Errores de mantenimiento / actualización de equipos (hardware)	2	3	3	3	MODERADO
5.3.17. [E.25] Pérdida de equipos	2	2	2	2	BAJO
5.4.4. [A.6] Abuso de privilegios de acceso	2	2	2	2	BAJO
5.4.9. [A.11] Acceso no autorizado	3	3	2	3	MODERADO
5.4.17. [A.23] Manipulación de los equipos	2	2	1	2	BAJO
5.4.19. [A.25] Robo	2	2	2	2	BAJO

- **HARDWARE- EQUIPOS INFORMÁTICOS: [HW_MV2]**

Tabla G.25. Valoración del riesgo potencial [HW_MV2]

[HW] HARDWARE- EQUIPOS INFORMÁTICOS					
[HW_MV2]	**Teléfonos móviles**				
AMENAZAS	**RIESGO POTENCIAL**				
	RIESGO POTENCIAL POR DIMENSIONES			**RIESGO POTENCIAL TOTAL**	
	Ri	**Rc**	**Rd**	**Rt**	**NIVEL**
5.1.1. [N.1] Fuego	2	3	3	3	MODERADO
5.1.2. [N.2] Daños por agua	2	3	3	3	MODERADO
5.2.3. [I.*] Desastres industriales	2	2	2	2	BAJO
5.2.6. [I.5] Avería de origen físico o lógico	2	3	3	3	MODERADO
5.2.7. [I.6] Corte del suministro eléctrico	2	3	4	3	MODERADO
5.3.1. [E.1] Errores de los usuarios	3	4	5	4	ALTO
5.3.2. [E.2] Errores del administrador	3	4	5	4	ALTO
5.3.12. [E.19] Fugas de información	5	5	5	5	MUY ALTO
5.3.15. [E.23] Errores de mantenimiento / actualización de equipos (hardware)	4	4	4	4	ALTO
5.3.17. [E.25] Pérdida de equipos	2	4	4	4	ALTO
5.4.3. [A.5] Suplantación de la identidad del usuario	2	3	3	3	MODERADO
5.4.4. [A.6] Abuso de privilegios de acceso	2	3	3	3	MODERADO
5.4.9. [A.11] Acceso no autorizado	2	3	2	3	MODERADO
5.4.17. [A.23] Manipulación de los equipos	3	4	4	4	ALTO
5.4.19. [A.25] Robo	4	4	4	4	ALTO

- **HARDWARE- EQUIPOS INFORMÁTICOS: [HW_PC]**

Tabla G.26. Valoración del Riesgo Potencial [HW_PC]

[HW] HARDWARE- EQUIPOS INFORMÁTICOS					
[HW_PC]	**Computadoras de escritorio**				
AMENAZAS	**RIESGO POTENCIAL**				
	RIESGO POTENCIAL POR DIMENSIONES			**RIESGO POTENCIAL TOTAL**	
	Ri	**Rc**	**Rd**	**Rt**	**NIVEL**
5.1.1. [N.1] Fuego	1	2	3	2	BAJO
5.1.2. [N.2] Daños por agua	2	2	3	3	MODERADO
5.2.3. [I.*] Desastres industriales	1	1	2	2	BAJO
5.2.6. [I.5] Avería de origen físico o lógico	2	2	3	3	MODERADO
5.2.7. [I.6] Corte del suministro eléctrico	3	4	4	4	ALTO
5.3.1. [E.1] Errores de los usuarios	4	4	4	4	ALTO
5.3.2. [E.2] Errores del administrador	4	4	4	4	ALTO
5.3.15. [E.23] Errores de mantenimiento / actualización de equipos (hardware)	3	4	4	4	ALTO
5.3.17. [E.25] Pérdida de equipos	4	4	4	4	ALTO
5.4.3. [A.5] Suplantación de la identidad del usuario	3	3	3	3	MODERADO
5.4.4. [A.6] Abuso de privilegios de acceso	2	3	2	3	MODERADO
5.4.9. [A.11] Acceso no autorizado	3	3	2	3	MODERADO
5.4.17. [A.23] Manipulación de los equipos	4	4	3	4	ALTO
5.4.19. [A.25] Robo	1	1	2	2	BAJO

- **HARDWARE- EQUIPOS INFORMÁTICOS: [HW_MV1]**

Tabla G.27. Valoración del Riesgo Potencial [HW_MV1]

[HW] HARDWARE- EQUIPOS INFORMÁTICOS					
[HW_MV1]	**Computadoras Portátiles**				
AMENAZAS	**RIESGO POTENCIAL**				
	RIESGO POTENCIAL POR DIMENSIONES			**RIESGO POTENCIAL TOTAL**	
	Ri	**Rc**	**Rd**	**Rt**	**NIVEL**
5.1.1. [N.1] Fuego	2	2	3	3	MODERADO
5.1.2. [N.2] Daños por agua	2	2	3	3	MODERADO
5.2.3. [I.*] Desastres industriales	1	1	2	2	BAJO
5.2.6. [I.5] Avería de origen físico o lógico	2	3	3	3	MODERADO
5.2.7. [I.6] Corte del suministro eléctrico	4	4	4	4	ALTO
5.3.1. [E.1] Errores de los usuarios	4	4	2	4	ALTO
5.3.2. [E.2] Errores del administrador	4	4	3	4	ALTO
5.3.15. [E.23] Errores de mantenimiento / actualización de equipos (hardware)	4	4	4	4	ALTO
5.3.17. [E.25] Pérdida de equipos	2	4	4	4	ALTO
5.4.3. [A.5] Suplantación de la identidad del usuario	3	3	3	3	MODERADO
5.4.4. [A.6] Abuso de privilegios de acceso	3	3	2	3	MODERADO
5.4.9. [A.11] Acceso no autorizado	2	3	2	3	MODERADO
5.4.17. [A.23] Manipulación de los equipos	4	4	3	4	ALTO
5.4.19. [A.25] Robo	4	4	4	4	ALTO

- **HARDWARE- EQUIPOS INFORMÁTICOS: [HW_WAP]**

Tabla G.28. Valoración del Riesgo Potencial [HW_WAP]

[HW] HARDWARE- EQUIPOS INFORMÁTICOS					
[HW_WAP]	**Punto de Acceso**				
AMENAZAS	**RIESGO POTENCIAL**				
	RIESGO POTENCIAL POR DIMENSIONES			**RIESGO POTENCIAL TOTAL**	
	Ri	**Rc**	**Rd**	**Rt**	**NIVEL**
5.1.1. [N.1] Fuego	2	2	2	2	BAJO
5.1.2. [N.2] Daños por agua	3	3	4	4	ALTO
5.2.3. [I.*] Desastres industriales	2	2	2	2	BAJO
5.2.6. [I.5] Avería de origen físico o lógico	2	3	3	3	MODERADO
5.2.7. [I.6] Corte del suministro eléctrico	4	4	4	4	ALTO
5.4.4. [A.6] Abuso de privilegios de acceso	2	3	2	3	MODERADO
5.4.9. [A.11] Acceso no autorizado	3	3	2	3	MODERADO
5.4.17. [A.23] Manipulación de los equipos	3	3	2	3	MODERADO
5.4.19. [A.25] Robo	2	2	2	2	BAJO

- **HARDWARE- EQUIPOS INFORMÁTICOS: [HW_PT]**

Tabla G.29. Valoración del Riesgo Potencial [HW_PT]

[HW] HARDWARE- EQUIPOS INFORMÁTICOS					
[HW_PT]	**Impresoras**				
AMENAZAS	**RIESGO POTENCIAL**				
	RIESGO POTENCIAL POR DIMENSIONES			**RIESGO POTENCIAL TOTAL**	
	Ri	**Rc**	**Rd**	**Rt**	**NIVEL**
5.1.1. [N.1] Fuego	1	1	1	1	MUY BAJO
5.1.2. [N.2] Daños por agua	1	1	2	2	BAJO
5.2.3. [I.*] Desastres industriales	1	1	1	1	MUY BAJO
5.2.6. [I.5] Avería de origen físico o lógico	1	2	2	2	BAJO
5.2.7. [I.6] Corte del suministro eléctrico	2	2	2	2	BAJO
5.4.4. [A.6] Abuso de privilegios de acceso	1	2	2	2	BAJO
5.4.9. [A.11] Acceso no autorizado	2	2	2	2	BAJO
5.4.17. [A.23] Manipulación de los equipos	2	2	2	2	BAJO
5.4.19. [A.25] Robo	1	1	1	1	MUY BAJO

- **REDES DE COMUNICACIONES: [Internet Fibra Óptica]**

Tabla G.30. Valoración del Riesgo Potencial [Internet Fibra Óptica]

[COM] REDES DE COMUNICACIONES					
Internet Fibra Óptica	**Internet Fibra Óptica**				
AMENAZAS	**RIESGO POTENCIAL**				
	RIESGO POTENCIAL POR DIMENSIONES			**RIESGO POTENCIAL TOTAL**	
	Ri	**Rc**	**Rd**	**Rt**	**NIVEL**
5.2.9. [I.8] Fallo de servicios de comunicaciones	2	4	5	4	ALTO
5.3.2. [E.2] Errores del administrador	3	4	4	4	ALTO
5.3.11. [E.18] Destrucción de información	1	2	2	2	BAJO
5.3.12. [E.19] Fugas de información	1	2	2	2	BAJO
5.4.3. [A.5] Suplantación de la identidad del usuario	2	3	2	3	MODERADO
5.4.4. [A.6] Abuso de privilegios de acceso	2	3	3	3	MODERADO
5.4.9. [A.11] Acceso no autorizado	2	4	4	4	ALTO
5.4.10. [A.12] Análisis de tráfico	4	4	3	4	ALTO
5.4.13. [A.15] Modificación deliberada de la información	2	2	2	2	BAJO
5.4.15. [A.19] Divulgación de información	1	2	2	2	BAJO
5.4.18. [A.24] Denegación de servicio	2	3	3	3	MODERADO

- **REDES DE COMUNICACIONES: [COM_LAN]**

Tabla G.31. Valoración del Riesgo Potencial [COM_LAN]

[COM] REDES DE COMUNICACIONES					
[COM_LAN]	**Red Local**				
AMENAZAS	**RIESGO POTENCIAL**				
	RIESGO POTENCIAL POR DIMENSIONES			**RIESGO POTENCIAL TOTAL**	
	Ri	**Rc**	**Rd**	**Rt**	**NIVEL**
5.2.9. [I.8] Fallo de servicios de comunicaciones	4	5	5	5	MUY ALTO
5.3.2. [E.2] Errores del administrador	4	4	4	4	ALTO
5.3.11. [E.18] Destrucción de información	2	2	2	2	BAJO
5.3.12. [E.19] Fugas de información	2	2	2	2	BAJO
5.4.3. [A.5] Suplantación de la identidad del usuario	2	3	2	3	MODERADO
5.4.4. [A.6] Abuso de privilegios de acceso	3	3	3	3	MODERADO
5.4.9. [A.11] Acceso no autorizado	3	4	4	4	ALTO
5.4.10. [A.12] Análisis de tráfico	4	4	4	4	ALTO
5.4.13. [A.15] Modificación deliberada de la información	3	3	3	3	MODERADO
5.4.15. [A.19] Divulgación de información	2	3	2	3	MODERADO
5.4.18. [A.24] Denegación de servicio	2	3	3	3	MODERADO

- **REDES DE COMUNICACIONES: [COM_MB]**

Tabla G.32. Valoración del Riesgo Potencial [COM_MB]

[COM] REDES DE COMUNICACIONES					
[COM_MB]	**Telefonía Móvil**				
AMENAZAS	**RIESGO POTENCIAL**				
	RIESGO POTENCIAL POR DIMENSIONES			**RIESGO POTENCIAL TOTAL**	
	Ri	**Rc**	**Rd**	**Rt**	**NIVEL**
5.2.9. [I.8] Fallo de servicios de comunicaciones	2	5	5	4	ALTO
5.3.2. [E.2] Errores del administrador	2	4	4	4	ALTO
5.3.11. [E.18] Destrucción de información	2	3	3	3	MODERADO
5.3.12. [E.19] Fugas de información	5	5	5	5	MUY ALTO
5.4.3. [A.5] Suplantación de la identidad del usuario	1	2	2	2	BAJO
5.4.4. [A.6] Abuso de privilegios de acceso	2	3	3	3	MODERADO
5.4.9. [A.11] Acceso no autorizado	2	5	4	4	ALTO
5.4.10. [A.12] Análisis de tráfico	1	2	2	2	BAJO
5.4.13. [A.15] Modificación deliberada de la información	2	2	2	2	BAJO
5.4.15. [A.19] Divulgación de información	5	5	3	5	MUY ALTO
5.4.18. [A.24] Denegación de servicio	2	3	3	3	MODERADO

- **REDES DE COMUNICACIONES: [COM_WF]**

Tabla G.33. Valoración del Riesgo Potencial [COM_WF]

[COM] REDES DE COMUNICACIONES					
[COM_WF]	**Red Inalámbrica**				
AMENAZAS	**RIESGO POTENCIAL**				
	RIESGO POTENCIAL POR DIMENSIONES			**RIESGO POTENCIAL TOTAL**	
	Ri	**Rc**	**Rd**	**Rt**	**NIVEL**
5.2.9. [I.8] Fallo de servicios de comunicaciones	2	4	4	4	ALTO
5.3.2. [E.2] Errores del administrador	2	4	4	4	ALTO
5.3.11. [E.18] Destrucción de información	1	1	3	2	BAJO
5.3.12. [E.19] Fugas de información	4	4	3	4	ALTO
5.4.3. [A.5] Suplantación de la identidad del usuario	2	3	2	3	MODERADO
5.4.4. [A.6] Abuso de privilegios de acceso	2	3	2	3	MODERADO
5.4.9. [A.11] Acceso no autorizado	3	4	4	4	ALTO
5.4.10. [A.12] Análisis de tráfico	2	2	2	2	BAJO
5.4.13. [A.15] Modificación deliberada de la información	2	2	1	2	BAJO
5.4.15. [A.19] Divulgación de información	4	4	3	4	ALTO
5.4.18. [A.24] Denegación de servicio	2	3	3	3	MODERADO

- **EQUIPO AUXILIAR: [AUX_CB]**

Tabla G.34. Valoración del Riesgo Potencial [AUX_CB]

[AUX] EQUIPO AUXILIAR					
[AUX_CB]	**Cableado Estructurado**				
AMENAZAS	**RIESGO POTENCIAL**				
	RIESGO POTENCIAL POR DIMENSIONES			**RIESGO POTENCIAL TOTAL**	
	Ri	**Rc**	**Rd**	**Rt**	**NIVEL**
5.1.1. [N.1] Fuego	1	1	2	2	BAJO
5.1.2. [N.2] Daños por agua	2	3	4	3	MODERADO
5.2.3. [I.*] Desastres industriales	1	1	2	2	BAJO
5.2.4. [I.3] Contaminación mecánica	2	2	4	3	MODERADO
5.2.6. [I.5] Avería de origen físico o lógico	2	2	3	3	MODERADO
5.2.7. [I.6] Corte del suministro eléctrico	3	2	5	4	ALTO
5.2.10. [I.9] Interrupción de otros servicios y suministros esenciales	2	3	5	4	ALTO
5.3.15. [E.23] Errores de mantenimiento / actualización de equipos (hardware)	3	3	3	3	MODERADO
5.3.17. [E.25] Pérdida de equipos	3	4	4	4	ALTO
5.4.9. [A.11] Acceso no autorizado	2	4	3	3	MODERADO
5.4.17. [A.23] Manipulación de los equipos	4	4	4	4	ALTO
5.4.19. [A.25] Robo	2	2	2	2	BAJO

- **EQUIPO AUXILIAR: [AUX_VIDEO]**

Tabla G.35. Valoración del Riesgo Potencial [AUX_VIDEO]

[AUX] EQUIPO AUXILIAR					
[AUX_VIDEO]	**Sistema de Video vigilancia**				
AMENAZAS	**RIESGO POTENCIAL**				
	RIESGO POTENCIAL POR DIMENSIONES			**RIESGO POTENCIAL TOTAL**	
	Ri	**Rc**	**Rd**	**Rt**	**NIVEL**
5.1.1. [N.1] Fuego	1	1	2	2	BAJO
5.1.2. [N.2] Daños por agua	2	3	4	3	MODERADO
5.2.3. [I.*] Desastres industriales	1	1	2	2	BAJO
5.2.4. [I.3] Contaminación mecánica	2	2	4	3	MODERADO
5.2.6. [I.5] Avería de origen físico o lógico	2	2	3	3	MODERADO
5.2.7. [I.6] Corte del suministro eléctrico	4	4	4	4	ALTO
5.2.10. [I.9] Interrupción de otros servicios y suministros esenciales	3	3	4	4	ALTO
5.3.15. [E.23] Errores de mantenimiento / actualización de equipos (hardware)	2	3	3	3	MODERADO
5.3.17. [E.25] Pérdida de equipos	1	3	4	3	MODERADO
5.4.9. [A.11] Acceso no autorizado	2	4	4	4	ALTO
5.4.17. [A.23] Manipulación de los equipos	3	3	3	3	MODERADO
5.4.19. [A.25] Robo	1	2	2	2	BAJO

- **EQUIPO AUXILIAR: [AUX_UPS]**

Tabla G.36. Valoración del Riesgo Potencial [AUX_UPS]

[AUX] EQUIPO AUXILIAR					
[AUX_UPS]	**Sistema de alimentación Interrumpida**				
AMENAZAS	**RIESGO POTENCIAL**				
	RIESGO POTENCIAL POR DIMENSIONES			**RIESGO POTENCIAL TOTAL**	
	Ri	**Rc**	**Rd**	**Rt**	**NIVEL**
5.1.1. [N.1] Fuego	1	1	2	2	BAJO
5.1.2. [N.2] Daños por agua	1	2	2	2	BAJO
5.2.3. [I.*] Desastres industriales	1	1	2	2	BAJO
5.2.4. [I.3] Contaminación mecánica	2	2	2	2	BAJO
5.2.6. [I.5] Avería de origen físico o lógico	2	2	2	2	BAJO
5.2.7. [I.6] Corte del suministro eléctrico	3	3	3	3	MODERADO
5.3.15. [E.23] Errores de mantenimiento / actualización de equipos (hardware)	1	2	2	2	BAJO
5.3.17. [E.25] Pérdida de equipos	2	2	2	2	BAJO
5.4.17. [A.23] Manipulación de los equipos	2	1	2	2	BAJO
5.4.19. [A.25] Robo	1	1	1	1	MUY BAJO

H. ANEXO H: ACEPTACIÓN Y TRATAMIENTO DEL RIESGO

- **INFORMACIÓN: [INFO_VR]**

Tabla H.1. Matriz de tratamiento del riesgo [INFO_VR]

[INFO] INFORMACIÓN					
[INFO_VR]	**Registros confidenciales de la organización**				
AMENAZAS	**RIESGO ACTUAL**		**TRATAMIENTO DEL RIESGO**	**CONTROLES/ SALVAGUARDAS SELECCIONADOS ***	
	Rt	**NIVEL**	**NIVEL**		
5.3.1. [E.1] Errores de los usuarios	4	ALTO	REDUCIR EL RIESGO	5.1.1	Políticas para la seguridad de la información.
5.3.2. [E.2] Errores del administrador	4	ALTO	REDUCIR EL RIESGO	6.1.5	Gestión de proyectos de seguridad de la información.
5.3.10. [E.15] Alteración accidental de la información	2	BAJO	ACEPTAR EL RIESGO	8.2.1	Clasificación de la información.
5.3.11. [E.18] Destrucción de información	2	BAJO	ACEPTAR EL RIESGO	9.1.1	Política de control de accesos.
5.3.12. [E.19] Fugas de información	2	BAJO	ACEPTAR EL RIESGO	13.2.1	Políticas y procedimientos de transferencia de información.
5.4.3. [A.5] Suplantación de la identidad del usuario	3	MODERADO	REDUCIR EL RIESGO	13.2.4	Acuerdos de confidencialidad o no revelación.
5.4.4. [A.6] Abuso de privilegios de acceso	2	BAJO	ACEPTAR EL RIESGO	16.1.5	Respuesta a incidentes de seguridad de la información.
5.4.9. [A.11] Acceso no autorizado	2	BAJO	ACEPTAR EL RIESGO	12.1.2	Gestión de cambios.
5.4.13. [A.15] Modificación deliberada de la información	2	BAJO	ACEPTAR EL RIESGO	17.1.1	Planificación de la continuidad de la seguridad de la información.
5.4.15. [A.19] Divulgación de información	3	MODERADO	REDUCIR EL RIESGO	18.1.2	Derechos de propiedad intelectual.

- **INFORMACIÓN: [INFO_PER]**

Tabla H.2. Matriz de tratamiento del riesgo [INFO_PER]

[INFO] INFORMACIÓN				
[INFO_PER]	**Base de datos de clientes y proveedores**			
AMENAZAS	**RIESGO ACTUAL**		**TRATAMIENTO DEL RIESGO**	**CONTROLES/ SALVAGUARDAS SELECCIONADOS ***
	Rt	**NIVEL**	**NIVEL**	
5.3.1. [E.1] Errores de los usuarios	3	MODERADO	REDUCIR EL RIESGO	5.1.1 Políticas para la seguridad de la información.
5.3.2. [E.2] Errores del administrador	4	ALTO	REDUCIR EL RIESGO	6.1.1 Roles y responsabilidades de seguridad de la información.
5.3.10. [E.15] Alteración accidental de la información	3	MODERADO	REDUCIR EL RIESGO	8.2.1 Clasificación de la información.
5.3.11. [E.18] Destrucción de información	3	MODERADO	REDUCIR EL RIESGO	9.1.1 Política de control de accesos.
5.3.12. [E.19] Fugas de información	4	ALTO	REDUCIR EL RIESGO	13.2.1 Políticas y procedimientos de transferencia de información.
5.4.3. [A.5] Suplantación de la identidad del usuario	3	MODERADO	REDUCIR EL RIESGO	13.2.4 Acuerdos de confidencialidad o no revelación.
5.4.4. [A.6] Abuso de privilegios de acceso	1	MUY BAJO	ACEPTAR EL RIESGO	16.1.5 Respuesta a incidentes de seguridad de la información.
5.4.9. [A.11] Acceso no autorizado	2	BAJO	ACEPTAR EL RIESGO	12.1.2 Gestión de cambios.
5.4.13. [A.15] Modificación deliberada de la información	1	MUY BAJO	ACEPTAR EL RIESGO	17.1.1 Planificación de la continuidad de la seguridad de la información.
5.4.15. [A.19] Divulgación de información	3	MODERADO	REDUCIR EL RIESGO	18.1.2 Derechos de propiedad intelectual.

- **INFORMACIÓN: [INFO_PUB]**

Tabla H.3. Matriz de tratamiento del riesgo [INFO_PUB]

[INFO] INFORMACIÓN				
[INFO_PUB]	**Documentación y permisos de funcionamiento**			
AMENAZAS	**RIESGO ACTUAL**		**TRATAMIENTO DEL RIESGO**	**CONTROLES/ SALVAGUARDAS SELECCIONADOS ***
	Rt	**NIVEL**	**NIVEL**	
5.3.1. [E.1] Errores de los usuarios	4	ALTO	REDUCIR EL RIESGO	5.1.1 Políticas para la seguridad de la información.
5.3.2. [E.2] Errores del administrador	4	ALTO	REDUCIR EL RIESGO	6.1.1 Roles y responsabilidades de seguridad de la información.
5.3.10. [E.15] Alteración accidental de la información	3	MODERADO	REDUCIR EL RIESGO	8.2.1 Clasificación de la información.
5.3.11. [E.18] Destrucción de información	2	BAJO	ACEPTAR EL RIESGO	9.1.1 Política de control de accesos.
5.3.12. [E.19] Fugas de información	1	MUY BAJO	ACEPTAR EL RIESGO	13.2.1 Políticas y procedimientos de transferencia de información.
5.4.3. [A.5] Suplantación de la identidad del usuario	2	BAJO	ACEPTAR EL RIESGO	13.2.4 Acuerdos de confidencialidad o no revelación.
5.4.4. [A.6] Abuso de privilegios de acceso	1	MUY BAJO	ACEPTAR EL RIESGO	16.1.5 Respuesta a incidentes de seguridad de la información.
5.4.9. [A.11] Acceso no autorizado	1	MUY BAJO	ACEPTAR EL RIESGO	12.1.2 Gestión de cambios.
5.4.13. [A.15] Modificación deliberada de la información	1	MUY BAJO	ACEPTAR EL RIESGO	17.1.1 Planificación de la continuidad de la seguridad de la información.
5.4.15. [A.19] Divulgación de información	2	BAJO	ACEPTAR EL RIESGO	18.1.2 Derechos de propiedad intelectual.

- **DATOS E INFORMACIÓN COMPLEMENTARIA: [D_BCK]**

Tabla H.4. Matriz de tratamiento del riesgo [D_BCK]

[D] DATOS E INFORMACIÓN COMPLEMENTARIA				
[D_BCK]	**Copias de seguridad *OwnCloud***			
AMENAZAS	**RIESGO ACTUAL**		**TRATAMIENTO DEL RIESGO**	**CONTROLES/ SALVAGUARDAS SELECCIONADOS ***
	Rt	**NIVEL**	**NIVEL**	
5.3.1. [E.1] Errores de los usuarios	1	MUY BAJO	ACEPTAR EL RIESGO	5.1.1 Políticas para la seguridad de la información.
5.3.2. [E.2] Errores del administrador	3	MODERADO	REDUCIR EL RIESGO	6.1.1 Roles y responsabilidades de seguridad de la información.
5.3.10. [E.15] Alteración accidental de la información	3	MODERADO	REDUCIR EL RIESGO	8.1.3 Uso aceptable de los activos.
5.3.11. [E.18] Destrucción de información	2	BAJO	ACEPTAR EL RIESGO	8.2.1 Clasificación de la información.
5.3.12. [E.19] Fugas de información	1	MUY BAJO	ACEPTAR EL RIESGO	8.3.1 Gestión de medios extraíbles.
5.4.3. [A.5] Suplantación de la identidad del usuario	3	MODERADO	REDUCIR EL RIESGO	9.1.1 Política de control de accesos.
5.4.4. [A.6] Abuso de privilegios de acceso	1	MUY BAJO	ACEPTAR EL RIESGO	9.4.1 Restricción del acceso a la información.
5.4.9. [A.11] Acceso no autorizado	2	BAJO	ACEPTAR EL RIESGO	12.3.1 Copias de seguridad de la información.
5.4.13. [A.15] Modificación deliberada de la información	1	MUY BAJO	ACEPTAR EL RIESGO	12.1.2 Gestión de cambios.
5.4.15. [A.19] Divulgación de información	2	BAJO	ACEPTAR EL RIESGO	13.2.4 Acuerdos de confidencialidad o no revelación.

- **DATOS E INFORMACIÓN COMPLEMENTARIA: [D_LG]**

Tabla H.5. Matriz de tratamiento del riesgo [D_LG]

[D] DATOS E INFORMACIÓN COMPLEMENTARIA				
[D_LG]	**Logs de SACI**			
AMENAZAS	**RIESGO ACTUAL**		**TRATAMIENTO DEL RIESGO**	**CONTROLES/ SALVAGUARDAS SELECCIONADOS ***
	Rt	**NIVEL**	**NIVEL**	
5.3.1. [E.1] Errores de los usuarios	3	MODERADO	REDUCIR EL RIESGO	5.1.1 Políticas para la seguridad de la información.
5.3.2. [E.2] Errores del administrador	3	MODERADO	REDUCIR EL RIESGO	6.1.1 Roles y responsabilidades de seguridad de la información.
5.3.3. [E.3] Errores de monitorización (log)	3	MODERADO	REDUCIR EL RIESGO	8.1.3 Uso aceptable de los activos.
5.3.10. [E.15] Alteración accidental de la información	3	MODERADO	REDUCIR EL RIESGO	8.2.1 Clasificación de la información.
5.3.11. [E.18] Destrucción de información	1	MUY BAJO	ACEPTAR EL RIESGO	8.2.2 Etiquetado de la información.
5.3.12. [E.19] Fugas de información	3	MODERADO	REDUCIR EL RIESGO	9.1.1 Política de control de accesos.
5.4.1. [A.3] Manipulación de los registros de actividad (log)	1	MUY BAJO	ACEPTAR EL RIESGO	9.1.2 Control de acceso a las redes y servicios asociados.
5.4.3. [A.5] Suplantación de la identidad del usuario	2	BAJO	ACEPTAR EL RIESGO	9.2.3 Gestión de privilegios de derechos de acceso.
5.4.4. [A.6] Abuso de privilegios de acceso	1	MUY BAJO	ACEPTAR EL RIESGO	12.1.2 Gestión de cambios.
5.4.9. [A.11] Acceso no autorizado	1	MUY BAJO	ACEPTAR EL RIESGO	12.3.1 Copias de seguridad de la información.
5.4.13. [A.15] Modificación deliberada de la información	1	MUY BAJO	ACEPTAR EL RIESGO	16.1.7 Recopilación de evidencias.
5.4.15. [A.19] Divulgación de información	1	MUY BAJO	ACEPTAR EL RIESGO	17.2.1 Disponibilidad de las instalaciones de procesamiento de la información.

- **CLAVES CRIPTOGRÁFICAS: [K_PB]**

Tabla H.6. Matriz de tratamiento del riesgo [K_PB]

[K] CLAVES CRIPTOGRÁFICAS				
[K_PB]	**SSL**			
AMENAZAS	**RIESGO ACTUAL**		**TRATAMIENTO DEL RIESGO**	**CONTROLES/ SALVAGUARDAS SELECCIONADOS ***
	Rt	**NIVEL**	**NIVEL**	
5.3.1. [E.1] Errores de los usuarios	2	BAJO	ACEPTAR EL RIESGO	5.1.1 Políticas para la seguridad de la información.
5.3.2. [E.2] Errores del administrador	3	MODERADO	REDUCIR EL RIESGO	6.1.4 Contacto con grupos de interés especial.
5.3.10. [E.15] Alteración accidental de la información	3	MODERADO	REDUCIR EL RIESGO	9.2.3 Gestión de privilegios de derechos de acceso.
5.3.11. [E.18] Destrucción de información	3	MODERADO	REDUCIR EL RIESGO	9.4.2 Procedimientos seguros de inicio de sesión.
5.3.12. [E.19] Fugas de información	1	MUY BAJO	ACEPTAR EL RIESGO	10.1.1 Política de uso de los controles criptográficos.
5.4.3. [A.5] Suplantación de la identidad del usuario	3	MODERADO	REDUCIR EL RIESGO	10.1.2 Gestión de Llaves.
5.4.4. [A.6] Abuso de privilegios de acceso	1	MUY BAJO	ACEPTAR EL RIESGO	12.3.1 Copias de seguridad de la información.
5.4.9. [A.11] Acceso no autorizado	2	BAJO	ACEPTAR EL RIESGO	12.6.1 Gestión de vulnerabilidades técnicas.
5.4.13. [A.15] Modificación deliberada de la información	1	MUY BAJO	ACEPTAR EL RIESGO	13.1.2 Seguridad de los servicios de red.
5.4.15. [A.19] Divulgación de información	1	MUY BAJO	ACEPTAR EL RIESGO	13.2.4 Acuerdos de confidencialidad o no revelación.

- **CLAVES CRIPTOGRÁFICAS: [K_SIGN]**

Tabla H.7. Matriz de tratamiento del riesgo [K_SIGN]

[K] CLAVES CRIPTOGRÁFICAS				
[K_SIGN]	**Token Digital**			
AMENAZAS	**RIESGO ACTUAL**		**TRATAMIENTO DEL RIESGO**	**CONTROLES/ SALVAGUARDAS SELECCIONADOS ***
	Rt	**NIVEL**	**NIVEL**	
5.3.1. [E.1] Errores de los usuarios	3	MODERADO	REDUCIR EL RIESGO	5.1.1 Políticas para la seguridad de la información.
5.3.2. [E.2] Errores del administrador	3	MODERADO	REDUCIR EL RIESGO	8.3.1 Gestión de medios extraíbles.
5.3.10. [E.15] Alteración accidental de la información	3	MODERADO	REDUCIR EL RIESGO	8.3.2 Eliminación de los medios.
5.3.11. [E.18] Destrucción de información	2	BAJO	ACEPTAR EL RIESGO	9.3.1 Uso de la información secreta de autenticación.
5.3.12. [E.19] Fugas de información	1	MUY BAJO	ACEPTAR EL RIESGO	10.1.1 Política de uso de los controles criptográficos.
5.4.3. [A.5] Suplantación de la identidad del usuario	3	MODERADO	REDUCIR EL RIESGO	10.1.2 Gestión de Llaves.
5.4.4. [A.6] Abuso de privilegios de acceso	1	MUY BAJO	ACEPTAR EL RIESGO	12.3.1 Copias de seguridad de la información.
5.4.9. [A.11] Acceso no autorizado	2	BAJO	ACEPTAR EL RIESGO	12.6.1 Gestión de vulnerabilidades técnicas.
5.4.13. [A.15] Modificación deliberada de la información	1	MUY BAJO	ACEPTAR EL RIESGO	13.1.2 Seguridad de los servicios de red.
5.4.15. [A.19] Divulgación de información	1	MUY BAJO	ACEPTAR EL RIESGO	13.2.4 Acuerdos de confidencialidad o no revelación.

- **SERVICIOS: [S_INT]**

Tabla H.8. Matriz de tratamiento del riesgo [S_INT]

[S] SERVICIOS				
[S_INT]	**Servicio del sistema contable**			
AMENAZAS	**RIESGO ACTUAL**		**TRATAMIENTO DEL RIESGO**	**CONTROLES/ SALVAGUARDAS SELECCIONADOS ***
	Rt	**NIVEL**	**NIVEL**	
5.3.1. [E.1] Errores de los usuarios	4	ALTO	REDUCIR EL RIESGO	5.1.1 Políticas para la seguridad de la información.
5.3.2. [E.2] Errores del administrador	4	ALTO	REDUCIR EL RIESGO	6.1.2 Separación de funciones.
5.3.10. [E.15] Alteración accidental de la información	3	MODERADO	REDUCIR EL RIESGO	6.1.4 Contacto con grupos de interés especial.
5.3.11. [E.18] Destrucción de información	2	BAJO	ACEPTAR EL RIESGO	9.2.2 Provisión de accesos a usuarios.
5.3.12. [E.19] Fugas de información	1	MUY BAJO	ACEPTAR EL RIESGO	9.2.1 Registro y retiro de usuario.
5.4.3. [A.5] Suplantación de la identidad del usuario	3	MODERADO	REDUCIR EL RIESGO	9.2.3 Gestión de privilegios de derechos de acceso.
5.4.4. [A.6] Abuso de privilegios de acceso	1	MUY BAJO	ACEPTAR EL RIESGO	9.2.4 Gestión de la información secreta de autenticación de los usuarios.
5.4.9. [A.11] Acceso no autorizado	2	BAJO	ACEPTAR EL RIESGO	13.1.2 Seguridad de los servicios de red.
5.4.13. [A.15] Modificación deliberada de la información	1	MUY BAJO	ACEPTAR EL RIESGO	16.1.1 Responsabilidades y procedimientos.
5.4.15. [A.19] Divulgación de información	1	MUY BAJO	ACEPTAR EL RIESGO	16.1.5 Respuesta a incidentes de seguridad de la información.

- **SERVICIOS: [S_WWW]**

Tabla H.9. Matriz de tratamiento del riesgo [S_WWW]

[S] SERVICIOS				
[S_WWW]	**Sitio web**			
AMENAZAS	**RIESGO ACTUAL**		**TRATAMIENTO DEL RIESGO**	**CONTROLES/ SALVAGUARDAS SELECCIONADOS ***
	Rt	**NIVEL**	**NIVEL**	
5.3.1. [E.1] Errores de los usuarios	4	ALTO	REDUCIR EL RIESGO	5.1.1 Políticas para la seguridad de la información.
5.3.2. [E.2] Errores del administrador	3	MODERADO	REDUCIR EL RIESGO	6.1.4 Contacto con grupos de interés especial.
5.3.10. [E.15] Alteración accidental de la información	4	ALTO	REDUCIR EL RIESGO	9.1.1 Política de control de accesos.
5.3.11. [E.18] Destrucción de información	2	BAJO	ACEPTAR EL RIESGO	9.1.2 Control de acceso a las redes y servicios asociados.
5.3.12. [E.19] Fugas de información	4	ALTO	REDUCIR EL RIESGO	9.2.5 Revisión de los derechos de acceso de usuario.
5.4.3. [A.5] Suplantación de la identidad del usuario	4	ALTO	REDUCIR EL RIESGO	9.2.6 Retiro y ajuste de los derechos de acceso.
5.4.4. [A.6] Abuso de privilegios de acceso	2	BAJO	ACEPTAR EL RIESGO	9.4.2 Procedimientos seguros de inicio de sesión.
5.4.9. [A.11] Acceso no autorizado	2	BAJO	ACEPTAR EL RIESGO	9.4.3 Sistema de gestión de contraseñas.
5.4.13. [A.15] Modificación deliberada de la información	1	MUY BAJO	ACEPTAR EL RIESGO	12.4.2 Protección de la información de registro.
5.4.15. [A.19] Divulgación de información	2	BAJO	ACEPTAR EL RIESGO	13.1.2 Seguridad de los servicios de red.
5.4.18. [A.24] Denegación de servicio	2	BAJO	ACEPTAR EL RIESGO	16.1.5 Respuesta a incidentes de seguridad de la información.

- **SOFTWARE- APLICACIONES INFORMÁTICAS: [SW_HP]**

Tabla H.10. Matriz de tratamiento del riesgo [SW_HP]

[SW] SOFTWARE- APLICACIONES INFORMÁTICAS				
[SW_HP]	**Proxmox**			
AMENAZAS	**RIESGO ACTUAL**		**TRATAMIENTO DEL RIESGO**	**CONTROLES/ SALVAGUARDAS SELECCIONADOS ***
	Rt	**NIVEL**	**NIVEL**	
5.2.6. [I.5] Avería de origen físico o lógico	4	ALTO	REDUCIR EL RIESGO	5.1.1 Políticas para la seguridad de la información.
5.3.1. [E.1] Errores de los usuarios	3	MODERADO	REDUCIR EL RIESGO	6.1.4 Contacto con grupos de interés especial.
5.3.2. [E.2] Errores del administrador	4	ALTO	REDUCIR EL RIESGO	9.4.2 Procedimientos seguros de inicio de sesión.
5.3.6. [E.8] Difusión de software dañino	2	BAJO	ACEPTAR EL RIESGO	12.1.1 Documentación de procedimientos de operación.
5.3.10. [E.15] Alteración accidental de la información	4	ALTO	REDUCIR EL RIESGO	12.2.1 Controles contra un malware.
5.3.11. [E.18] Destrucción de información	4	ALTO	REDUCIR EL RIESGO	12.4.3 Registros de administración y operación.
5.3.12. [E.19] Fugas de información	2	BAJO	ACEPTAR EL RIESGO	12.4.4 Sincronización del reloj.
5.3.13. [E.20] Vulnerabilidades de los programas (software)	2	BAJO	ACEPTAR EL RIESGO	12.6.1 Gestión de vulnerabilidades técnicas.
5.3.14. [E.21] Errores de mantenimiento / actualización de programas	1	MUY BAJO	ACEPTAR EL RIESGO	13.1.2 Seguridad de los servicios de red.
5.4.3. [A.5] Suplantación de la identidad del usuario	2	BAJO	ACEPTAR EL RIESGO	13.2.1 Políticas y procedimientos de transferencia de información.
5.4.4. [A.6] Abuso de privilegios de acceso	2	BAJO	ACEPTAR EL RIESGO	13.2.4 Acuerdos de confidencialidad o no revelación.
5.4.9. [A.11] Acceso no autorizado	1	MUY BAJO	ACEPTAR EL RIESGO	13.2.4 Acuerdos de confidencialidad o no revelación.
5.4.13. [A.15] Modificación deliberada de la información	2	BAJO	ACEPTAR EL RIESGO	16.1.3 Informe de debilidades de seguridad de la información.
5.4.15. [A.19] Divulgación de información	2	BAJO	ACEPTAR EL RIESGO	16.1.4 Apreciación y decisión sobre los eventos de seguridad de la información.
5.4.16. [A.22] Manipulación de programas	2	BAJO	ACEPTAR EL RIESGO	16.1.5 Respuesta a incidentes de seguridad de la información.
5.4.18. [A.24] Denegación de servicio	2	BAJO	ACEPTAR EL RIESGO	17.1.1 Planificación de la continuidad de la seguridad de la información.

- **SOFTWARE- APLICACIONES INFORMÁTICAS: [SW_BD1]**

Tabla H.11. Matriz de tratamiento del riesgo [SW_BD1]

[SW] SOFTWARE- APLICACIONES INFORMÁTICAS				
[SW_BD1] Servidor de Base de Datos Oracle XE 18c				
AMENAZAS	**RIESGO ACTUAL**		**TRATAMIENTO DEL RIESGO**	**CONTROLES/ SALVAGUARDAS SELECCIONADOS ***
	Rt	**NIVEL**	**NIVEL**	
5.2.6. [I.5] Avería de origen físico o lógico	2	BAJO	ACEPTAR EL RIESGO	5.1.1 Políticas para la seguridad de la información.
5.3.1. [E.1] Errores de los usuarios	3	MODERADO	REDUCIR EL RIESGO	6.1.1 Roles y responsabilidades de seguridad de la información.
5.3.2. [E.2] Errores del administrador	3	MODERADO	REDUCIR EL RIESGO	6.1.4 Contacto con grupos de interés especial.
5.3.6. [E.8] Difusión de software dañino	3	MODERADO	REDUCIR EL RIESGO	8.2.1 Clasificación de la información.
5.3.10. [E.15] Alteración accidental de la información	2	BAJO	ACEPTAR EL RIESGO	9.1.1 Política de control de accesos.
5.3.11. [E.18] Destrucción de información	2	BAJO	ACEPTAR EL RIESGO	9.4.2 Procedimientos seguros de inicio de sesión.
5.3.12. [E.19] Fugas de información	2	BAJO	ACEPTAR EL RIESGO	12.1.4 Separación de ambientes de desarrollo, pruebas y producción.
5.4.3. [A.5] Suplantación de la identidad del usuario	1	MUY BAJO	ACEPTAR EL RIESGO	12.3.1 Copias de seguridad de la información.
5.4.9. [A.11] Acceso no autorizado	1	MUY BAJO	ACEPTAR EL RIESGO	12.4.3 Registros de administración y operación.
5.4.13. [A.15] Modificación deliberada de la información	2	BAJO	ACEPTAR EL RIESGO	13.2.4 Acuerdos de confidencialidad o no revelación.
5.4.15. [A.19] Divulgación de información	2	BAJO	ACEPTAR EL RIESGO	17.1.1 Planificación de la continuidad de la seguridad de la información.
5.4.18. [A.24] Denegación de servicio	2	BAJO	ACEPTAR EL RIESGO	18.1.2 Derechos de propiedad intelectual.

- **SOFTWARE- APLICACIONES INFORMÁTICAS: [SW_APP4]**

Tabla H.12. Matriz de tratamiento del riesgo [SW_APP4]

[SW] SOFTWARE- APLICACIONES INFORMÁTICAS				
[SW_APP4]	**Servidor Digital Ocean**			
AMENAZAS	**RIESGO ACTUAL**		**TRATAMIENTO DEL RIESGO**	**CONTROLES/ SALVAGUARDAS SELECCIONADOS ***
	Rt	**NIVEL**	**NIVEL**	
5.2.6. [I.5] Avería de origen físico o lógico	2	BAJO	ACEPTAR EL RIESGO	5.1.1 Políticas para la seguridad de la información.
5.3.2. [E.2] Errores del administrador	3	MODERADO	REDUCIR EL RIESGO	6.1.4 Contacto con grupos de interés especial.
5.3.6. [E.8] Difusión de software dañino	3	MODERADO	REDUCIR EL RIESGO	9.2.3 Gestión de privilegios de derechos de acceso.
5.4.3. [A.5] Suplantación de la identidad del usuario	3	MODERADO	REDUCIR EL RIESGO	13.2.1 Políticas y procedimientos de transferencia de información.
5.4.4. [A.6] Abuso de privilegios de acceso	2	BAJO	ACEPTAR EL RIESGO	16.1.5 Respuesta a incidentes de seguridad de la información.
5.4.9. [A.11] Acceso no autorizado	2	BAJO	ACEPTAR EL RIESGO	17.1.1 Planificación de la continuidad de la seguridad de la información.

- **SOFTWARE- APLICACIONES INFORMÁTICAS: [SW_APP2]**

Tabla H.13. Matriz de tratamiento del riesgo [SW_APP2]

[SW] SOFTWARE- APLICACIONES INFORMÁTICAS				
[SW_APP2]	**Servidor FTP**			
AMENAZAS	**RIESGO ACTUAL**		**TRATAMIENTO DEL RIESGO**	**CONTROLES/ SALVAGUARDAS SELECCIONADOS ***
	Rt	**NIVEL**	**NIVEL**	
5.2.6. [I.5] Avería de origen físico o lógico	3	MODERADO	REDUCIR EL RIESGO	5.1.1 Políticas para la seguridad de la información.
5.3.2. [E.2] Errores del administrador	2	BAJO	ACEPTAR EL RIESGO	6.1.4 Contacto con grupos de interés especial.
5.3.6. [E.8] Difusión de software dañino	3	MODERADO	REDUCIR EL RIESGO	9.2.3 Gestión de privilegios de derechos de acceso.
5.3.10. [E.15] Alteración accidental de la información	2	BAJO	ACEPTAR EL RIESGO	12.1.4 Separación de ambientes de desarrollo, pruebas y producción.
5.3.11. [E.18] Destrucción de información	1	MUY BAJO	ACEPTAR EL RIESGO	12.6.1 Gestión de vulnerabilidades técnicas.
5.4.3. [A.5] Suplantación de la identidad del usuario	2	BAJO	ACEPTAR EL RIESGO	13.1.2 Seguridad de los servicios de red.
5.4.4. [A.6] Abuso de privilegios de acceso	3	MODERADO	REDUCIR EL RIESGO	13.2.1 Políticas y procedimientos de transferencia de información.
5.4.9. [A.11] Acceso no autorizado	2	BAJO	ACEPTAR EL RIESGO	16.1.5 Respuesta a incidentes de seguridad de la información.
5.4.18. [A.24] Denegación de servicio	1	MUY BAJO	ACEPTAR EL RIESGO	17.1.1 Planificación de la continuidad de la seguridad de la información.

- **SOFTWARE- APLICACIONES INFORMÁTICAS: [SW_BD2]**

Tabla H.14. Matriz de tratamiento del riesgo [SW_BD2]

[SW] SOFTWARE- APLICACIONES INFORMÁTICAS				
[SW_BD2] Servidor de Base de Datos MySQL 8.0				
AMENAZAS	**RIESGO ACTUAL**		**TRATAMIENTO DEL RIESGO**	**CONTROLES/ SALVAGUARDAS SELECCIONADOS ***
	Rt	**NIVEL**	**NIVEL**	
5.2.6. [I.5] Avería de origen físico o lógico	3	MODERADO	REDUCIR EL RIESGO	5.1.1 Políticas para la seguridad de la información.
5.3.1. [E.1] Errores de los usuarios	3	MODERADO	REDUCIR EL RIESGO	6.1.1 Roles y responsabilidades de seguridad de la información.
5.3.2. [E.2] Errores del administrador	3	MODERADO	REDUCIR EL RIESGO	6.1.4 Contacto con grupos de interés especial.
5.3.6. [E.8] Difusión de software dañino	3	MODERADO	REDUCIR EL RIESGO	8.2.1 Clasificación de la información.
5.3.10. [E.15] Alteración accidental de la información	2	BAJO	ACEPTAR EL RIESGO	9.1.1 Política de control de accesos.
5.3.11. [E.18] Destrucción de información	1	MUY BAJO	ACEPTAR EL RIESGO	9.4.2 Procedimientos seguros de inicio de sesión.
5.3.12. [E.19] Fugas de información	2	BAJO	ACEPTAR EL RIESGO	12.1.4 Separación de ambientes de desarrollo, pruebas y producción.
5.4.3. [A.5] Suplantación de la identidad del usuario	1	MUY BAJO	ACEPTAR EL RIESGO	12.3.1 Copias de seguridad de la información.
5.4.9. [A.11] Acceso no autorizado	3	MODERADO	REDUCIR EL RIESGO	12.4.3 Registros de administración y operación.
5.4.13. [A.15] Modificación deliberada de la información	3	MODERADO	REDUCIR EL RIESGO	13.2.4 Acuerdos de confidencialidad o no revelación.
5.4.15. [A.19] Divulgación de información	2	BAJO	ACEPTAR EL RIESGO	17.1.1 Planificación de la continuidad de la seguridad de la información.
5.4.18. [A.24] Denegación de servicio	2	BAJO	ACEPTAR EL RIESGO	18.1.2 Derechos de propiedad intelectual.

- **SOFTWARE- APLICACIONES INFORMÁTICAS: [SW_APP3]**

Tabla H.15. Matriz de tratamiento del riesgo [SW_APP3]

[SW] SOFTWARE- APLICACIONES INFORMÁTICAS				
[SW_APP3]	**Servidor DNS**			
AMENAZAS	**RIESGO ACTUAL**		**TRATAMIENTO DEL RIESGO**	**CONTROLES/ SALVAGUARDAS SELECCIONADOS ***
	Rt	**NIVEL**	**NIVEL**	
5.2.6. [I.5] Avería de origen físico o lógico	3	MODERADO	REDUCIR EL RIESGO	5.1.1 Políticas para la seguridad de la información.
5.3.2. [E.2] Errores del administrador	3	MODERADO	REDUCIR EL RIESGO	6.1.4 Contacto con grupos de interés especial.
5.3.6. [E.8] Difusión de software dañino	3	MODERADO	REDUCIR EL RIESGO	9.2.3 Gestión de privilegios de derechos de acceso.
5.4.3. [A.5] Suplantación de la identidad del usuario	2	BAJO	ACEPTAR EL RIESGO	13.2.1 Políticas y procedimientos de transferencia de información.
5.4.4. [A.6] Abuso de privilegios de acceso	3	MODERADO	REDUCIR EL RIESGO	16.1.5 Respuesta a incidentes de seguridad de la información.
5.4.9. [A.11] Acceso no autorizado	2	BAJO	ACEPTAR EL RIESGO	17.1.1 Planificación de la continuidad de la seguridad de la información.
5.4.18. [A.24] Denegación de servicio	2	BAJO	ACEPTAR EL RIESGO	

- **SOFTWARE- APLICACIONES INFORMÁTICAS: [SW_BD3]**

Tabla H.16. Matriz de tratamiento del riesgo [SW_BD3]

[SW] SOFTWARE- APLICACIONES INFORMÁTICAS				
[SW_BD3]	**Servidor de Base de Datos Postgresql 13**			
AMENAZAS	**RIESGO ACTUAL**		**TRATAMIENTO DEL RIESGO**	**CONTROLES/ SALVAGUARDAS SELECCIONADOS ***
	Rt	**NIVEL**	**NIVEL**	
5.2.6. [I.5] Avería de origen físico o lógico	3	MODERADO	REDUCIR EL RIESGO	5.1.1 Políticas para la seguridad de la información.
5.3.1. [E.1] Errores de los usuarios	3	MODERADO	REDUCIR EL RIESGO	6.1.1 Roles y responsabilidades de seguridad de la información.
5.3.2. [E.2] Errores del administrador	3	MODERADO	REDUCIR EL RIESGO	6.1.4 Contacto con grupos de interés especial.
5.3.6. [E.8] Difusión de software dañino	3	MODERADO	REDUCIR EL RIESGO	8.2.1 Clasificación de la información.
5.3.10. [E.15] Alteración accidental de la información	4	ALTO	REDUCIR EL RIESGO	9.1.1 Política de control de accesos.
5.3.11. [E.18] Destrucción de información	2	BAJO	ACEPTAR EL RIESGO	9.4.2 Procedimientos seguros de inicio de sesión.
5.3.12. [E.19] Fugas de información	2	BAJO	ACEPTAR EL RIESGO	12.1.4 Separación de ambientes de desarrollo, pruebas y producción.
5.4.3. [A.5] Suplantación de la identidad del usuario	1	MUY BAJO	ACEPTAR EL RIESGO	12.3.1 Copias de seguridad de la información.
5.4.9. [A.11] Acceso no autorizado	2	BAJO	ACEPTAR EL RIESGO	12.4.3 Registros de administración y operación.
5.4.13. [A.15] Modificación deliberada de la información	3	MODERADO	REDUCIR EL RIESGO	13.2.4 Acuerdos de confidencialidad o no revelación.
5.4.15. [A.19] Divulgación de información	2	BAJO	ACEPTAR EL RIESGO	17.1.1 Planificación de la continuidad de la seguridad de la información.
5.4.18. [A.24] Denegación de servicio	2	BAJO	ACEPTAR EL RIESGO	18.1.2 Derechos de propiedad intelectual.

- **SOFTWARE- APLICACIONES INFORMÁTICAS: [SW_AV]**

Tabla H.17. Matriz de tratamiento del riesgo [SW_AV]

[SW] SOFTWARE- APLICACIONES INFORMÁTICAS				
[SW_AV] Avast Free Antivirus				
AMENAZAS	**RIESGO ACTUAL**		**TRATAMIENTO DEL RIESGO**	**CONTROLES/ SALVAGUARDAS SELECCIONADOS ***
	Rt	**NIVEL**	**NIVEL**	
5.2.6. [I.5] Avería de origen físico o lógico	3	MODERADO	REDUCIR EL RIESGO	5.1.1 Políticas para la seguridad de la información.
5.3.1. [E.1] Errores de los usuarios	3	MODERADO	REDUCIR EL RIESGO	9.2.3 Gestión de privilegios de derechos de acceso.
5.3.2. [E.2] Errores del administrador	3	MODERADO	REDUCIR EL RIESGO	9.4.1 Restricción del acceso a la información.
5.3.6. [E.8] Difusión de software dañino	3	MODERADO	REDUCIR EL RIESGO	12.2.1 Controles contra un malware.
5.3.13. [E.20] Vulnerabilidades de los programas (software)	3	MODERADO	REDUCIR EL RIESGO	12.4.2 Protección de la información de registro.
5.3.14. [E.21] Errores de mantenimiento / actualización de programas (software)	3	MODERADO	REDUCIR EL RIESGO	12.6.2 Restricciones en la instalación del software.
5.4.3. [A.5] Suplantación de la identidad del usuario	2	BAJO	ACEPTAR EL RIESGO	13.2.1 Políticas y procedimientos de transferencia de información.
5.4.4. [A.6] Abuso de privilegios de acceso	3	MODERADO	REDUCIR EL RIESGO	16.1.2 Informe de los eventos de seguridad de la información.
5.4.9. [A.11] Acceso no autorizado	2	BAJO	ACEPTAR EL RIESGO	17.1.1 Planificación de la continuidad de la seguridad de la información.

- **SOFTWARE- APLICACIONES INFORMÁTICAS: [SW_APP1]**

Tabla H.18. Matriz de tratamiento del riesgo [SW_APP1]

[SW] SOFTWARE- APLICACIONES INFORMÁTICAS				
[SW_APP1]	**Servidor de OwnCloud**			
AMENAZAS	**RIESGO ACTUAL**		**TRATAMIENTO DEL RIESGO**	**CONTROLES/ SALVAGUARDAS SELECCIONADOS ***
	Rt	**NIVEL**	**NIVEL**	
5.2.6. [I.5] Avería de origen físico o lógico	3	MODERADO	REDUCIR EL RIESGO	5.1.1 Políticas para la seguridad de la información.
5.3.1. [E.1] Errores de los usuarios	3	MODERADO	REDUCIR EL RIESGO	6.1.1 Roles y responsabilidades de seguridad de la información.
5.3.2. [E.2] Errores del administrador	3	MODERADO	REDUCIR EL RIESGO	6.1.4 Contacto con grupos de interés especial.
5.3.6. [E.8] Difusión de software dañino	3	MODERADO	REDUCIR EL RIESGO	8.2.1 Clasificación de la información.
5.3.10. [E.15] Alteración accidental de la información	3	MODERADO	REDUCIR EL RIESGO	9.1.1 Política de control de accesos.
5.3.11. [E.18] Destrucción de información	1	MUY BAJO	ACEPTAR EL RIESGO	9.4.2 Procedimientos seguros de inicio de sesión.
5.3.12. [E.19] Fugas de información	2	BAJO	ACEPTAR EL RIESGO	12.1.2 Gestión de cambios.
5.3.14. [E.21] Errores de mantenimiento / actualización de programas (software)	3	MODERADO	REDUCIR EL RIESGO	12.3.1 Copias de seguridad de la información.
5.4.3. [A.5] Suplantación de la identidad del usuario	2	BAJO	ACEPTAR EL RIESGO	12.4.3 Registros de administración y operación.
5.4.4. [A.6] Abuso de privilegios de acceso	4	ALTO	REDUCIR EL RIESGO	13.2.1 Políticas y procedimientos de transferencia de información.
5.4.9. [A.11] Acceso no autorizado	2	BAJO	ACEPTAR EL RIESGO	13.2.4 Acuerdos de confidencialidad o no revelación.
5.4.13. [A.15] Modificación deliberada de la información	3	MODERADO	REDUCIR EL RIESGO	16.1.5 Respuesta a incidentes de seguridad de la información.
5.4.15. [A.19] Divulgación de información	2	BAJO	ACEPTAR EL RIESGO	17.1.1 Planificación de la continuidad de la seguridad de la información.
5.4.18. [A.24] Denegación de servicio	2	BAJO	ACEPTAR EL RIESGO	18.1.2 Derechos de propiedad intelectual.

- **SOFTWARE- APLICACIONES INFORMÁTICAS: [SW_WWW]**

Tabla H.19. Matriz de tratamiento del riesgo [SW_WWW]

[SW] SOFTWARE- APLICACIONES INFORMÁTICAS				
[SW_WWW]	**Servidor Web NGINX**			
AMENAZAS	**RIESGO ACTUAL**		**TRATAMIENTO DEL RIESGO**	**CONTROLES/ SALVAGUARDAS SELECCIONADOS ***
	Rt	**NIVEL**	**NIVEL**	
5.2.6. [I.5] Avería de origen físico o lógico	2	BAJO	ACEPTAR EL RIESGO	5.1.1 Políticas para la seguridad de la información.
5.3.2. [E.2] Errores del administrador	2	BAJO	ACEPTAR EL RIESGO	6.1.4 Contacto con grupos de interés especial.
5.3.6. [E.8] Difusión de software dañino	2	BAJO	ACEPTAR EL RIESGO	9.2.3 Gestión de privilegios de derechos de acceso.
5.4.3. [A.5] Suplantación de la identidad del usuario	1	MUY BAJO	ACEPTAR EL RIESGO	13.2.1 Políticas y procedimientos de transferencia de información.
5.4.4. [A.6] Abuso de privilegios de acceso	2	BAJO	ACEPTAR EL RIESGO	16.1.5 Respuesta a incidentes de seguridad de la información.
5.4.9. [A.11] Acceso no autorizado	1	MUY BAJO	ACEPTAR EL RIESGO	17.1.1 Planificación de la continuidad de la seguridad de la información.
5.4.18. [A.24] Denegación de servicio	1	MUY BAJO	ACEPTAR EL RIESGO	

- **SOFTWARE- APLICACIONES INFORMÁTICAS: [SW_OS]**

Tabla H.20. Matriz de tratamiento del riesgo [SW_OS]

[SW] SOFTWARE- APLICACIONES INFORMÁTICAS				
[SW_OS]	**Windows/Linux**			
AMENAZAS	**RIESGO ACTUAL**		**TRATAMIENTO DEL RIESGO**	**CONTROLES/ SALVAGUARDAS SELECCIONADOS ***
	Rt	**NIVEL**	**NIVEL**	
5.2.6. [I.5] Avería de origen físico o lógico	2	BAJO	ACEPTAR EL RIESGO	5.1.1 Políticas para la seguridad de la información.
5.3.1. [E.1] Errores de los usuarios	3	MODERADO	REDUCIR EL RIESGO	6.1.1 Roles y responsabilidades de seguridad de la información.
5.3.2. [E.2] Errores del administrador	3	MODERADO	REDUCIR EL RIESGO	6.1.4 Contacto con grupos de interés especial.
5.3.6. [E.8] Difusión de software dañino	3	MODERADO	REDUCIR EL RIESGO	9.1.2 Control de acceso a las redes y servicios asociados.
5.3.10. [E.15] Alteración accidental de la información	1	MUY BAJO	ACEPTAR EL RIESGO	9.1.1 Política de control de accesos.
5.3.11. [E.18] Destrucción de información	1	MUY BAJO	ACEPTAR EL RIESGO	9.4.2 Procedimientos seguros de inicio de sesión.
5.3.12. [E.19] Fugas de información	2	BAJO	ACEPTAR EL RIESGO	12.2.1 Controles contra un malware.
5.3.13. [E.20] Vulnerabilidades de los programas (software)	4	ALTO	REDUCIR EL RIESGO	12.4.1 Registro de eventos.
5.3.14. [E.21] Errores de mantenimiento / actualización de programas (software)	3	MODERADO	REDUCIR EL RIESGO	12.5.1 Instalación del software en los sistemas operativos.
5.4.3. [A.5] Suplantación de la identidad del usuario	2	BAJO	ACEPTAR EL RIESGO	12.6.1 Gestión de vulnerabilidades técnicas.
5.4.4. [A.6] Abuso de privilegios de acceso	3	MODERADO	REDUCIR EL RIESGO	12.6.2 Restricciones en la instalación del software.
5.4.9. [A.11] Acceso no autorizado	3	MODERADO	REDUCIR EL RIESGO	12.7.1 Controles de auditoría de los sistemas de información.
5.4.13. [A.15] Modificación deliberada de la información	3	MODERADO	REDUCIR EL RIESGO	16.1.5 Respuesta a incidentes de seguridad de la información.
5.4.15. [A.19] Divulgación de información	2	BAJO	ACEPTAR EL RIESGO	17.1.1 Planificación de la continuidad de la seguridad de la información.
5.4.18. [A.24] Denegación de servicio	2	BAJO	ACEPTAR EL RIESGO	17.1.2 Implementación de la continuidad de seguridad de la información.

- **SOFTWARE- APLICACIONES INFORMÁTICAS: [SW_ALM]**

Tabla H.21. Matriz de tratamiento del riesgo [SW_ALM]

[SW] SOFTWARE- APLICACIONES INFORMÁTICAS				
[SW_ALM]	**Google Drive**			
AMENAZAS	**RIESGO ACTUAL**		**TRATAMIENTO DEL RIESGO**	**CONTROLES/ SALVAGUARDAS SELECCIONADOS ***
	Rt	**NIVEL**	**NIVEL**	
5.3.1. [E.1] Errores de los usuarios	2	BAJO	ACEPTAR EL RIESGO	5.1.1 Políticas para la seguridad de la información.
5.3.2. [E.2] Errores del administrador	2	BAJO	ACEPTAR EL RIESGO	8.2.1 Clasificación de la información.
5.3.10. [E.15] Alteración accidental de la información	1	MUY BAJO	ACEPTAR EL RIESGO	8.2.2 Etiquetado de la información.
5.3.11. [E.18] Destrucción de información	1	MUY BAJO	ACEPTAR EL RIESGO	9.1.1 Política de control de accesos.
5.3.12. [E.19] Fugas de información	2	BAJO	ACEPTAR EL RIESGO	9.2.3 Gestión de privilegios de derechos de acceso.
5.4.3. [A.5] Suplantación de la identidad del usuario	2	BAJO	ACEPTAR EL RIESGO	12.3.1 Copias de seguridad de la información.
5.4.4. [A.6] Abuso de privilegios de acceso	3	MODERADO	REDUCIR EL RIESGO	12.4.2 Protección de la información de registro.
5.4.9. [A.11] Acceso no autorizado	2	BAJO	ACEPTAR EL RIESGO	13.1.2 Seguridad de los servicios de red.
5.4.13. [A.15] Modificación deliberada de la información	2	BAJO	ACEPTAR EL RIESGO	16.1.5 Respuesta a incidentes de seguridad de la información.
5.4.15. [A.19] Divulgación de información	3	MODERADO	REDUCIR EL RIESGO	17.1.1 Planificación de la continuidad de la seguridad de la información.
5.4.18. [A.24] Denegación de servicio	2	BAJO	ACEPTAR EL RIESGO	

- **SOFTWARE- APLICACIONES INFORMÁTICAS: [SW_OFF]**

Tabla H.22. Matriz de tratamiento del riesgo [SW_OFF]

[SW] SOFTWARE- APLICACIONES INFORMÁTICAS					
[SW_OFF]	Microsoft Office Professional 2019				
AMENAZAS	**RIESGO ACTUAL**		**TRATAMIENTO DEL RIESGO**	**CONTROLES/ SALVAGUARDAS SELECCIONADOS ***	
	Rt	**NIVEL**	**NIVEL**		
5.2.6. [I.5] Avería de origen físico o lógico	2	BAJO	ACEPTAR EL RIESGO	5.1.1	Políticas para la seguridad de la información.
5.3.1. [E.1] Errores de los usuarios	1	MUY BAJO	ACEPTAR EL RIESGO	9.1.2	Control de acceso a las redes y servicios asociados.
5.3.2. [E.2] Errores del administrador	1	MUY BAJO	ACEPTAR EL RIESGO	9.4.2	Procedimientos seguros de inicio de sesión.
5.3.6. [E.8] Difusión de software dañino	2	BAJO	ACEPTAR EL RIESGO	12.4.1	Registro de eventos.
5.3.14. [E.21] Errores de mantenimiento / actualización de programas (software)	1	MUY BAJO	ACEPTAR EL RIESGO	12.5.1	Instalación del software en los sistemas operativos.
5.4.3. [A.5] Suplantación de la identidad del usuario	2	BAJO	ACEPTAR EL RIESGO	12.6.1	Gestión de vulnerabilidades técnicas.
5.4.4. [A.6] Abuso de privilegios de acceso	2	BAJO	ACEPTAR EL RIESGO	12.6.2	Restricciones en la instalación del software.
5.4.9. [A.11] Acceso no autorizado	2	BAJO	ACEPTAR EL RIESGO	13.1.2	Seguridad de los servicios de red.
5.4.18. [A.24] Denegación de servicio	1	MUY BAJO	ACEPTAR EL RIESGO	16.1.5	Respuesta a incidentes de seguridad de la información.

- **[HW] HARDWARE - EQUIPOS INFORMÁTICOS: [HW_HT]**

Tabla H.23. Matriz de tratamiento del riesgo [HW_HT]

[HW] HARDWARE- EQUIPOS INFORMÁTICOS				
[HW_HT]	**Servidor físico HP Proliant DL 360P**			
AMENAZAS	**RIESGO ACTUAL**		**TRATAMIENTO DEL RIESGO**	**CONTROLES/ SALVAGUARDAS SELECCIONADOS ***
	Rt	**NIVEL**	**NIVEL**	
5.1.1. [N.1] Fuego	2	BAJO	ACEPTAR EL RIESGO	5.1.1 Políticas para la seguridad de la información.
5.1.2. [N.2] Daños por agua	2	BAJO	ACEPTAR EL RIESGO	5.1.2 Revisión de las políticas para la seguridad de la información.
5.2.3. [I.*] Desastres industriales	1	MUY BAJO	ACEPTAR EL RIESGO	6.1.1 Roles y responsabilidades de seguridad de la información.
5.2.6. [I.5] Avería de origen físico o lógico	3	MODERADO	REDUCIR EL RIESGO	8.1.2 Propiedad de los activos.
5.2.7. [I.6] Corte del suministro eléctrico	4	ALTO	REDUCIR EL RIESGO	8.3.1 Gestión de medios extraíbles.
5.3.2. [E.2] Errores del administrador	4	ALTO	REDUCIR EL RIESGO	8.3.3 Transferencia de medios físicos.
5.3.15. [E.23] Errores de mantenimiento / actualización de equipos (hardware)	2	BAJO	ACEPTAR EL RIESGO	9.1.1 Política de control de accesos.
5.3.17. [E.25] Pérdida de equipos	2	BAJO	ACEPTAR EL RIESGO	12.1.3 Gestión de capacidades.
5.4.4. [A.6] Abuso de privilegios de acceso	1	MUY BAJO	ACEPTAR EL RIESGO	12.4.3 Registros de administración y operación.
5.4.9. [A.11] Acceso no autorizado	2	BAJO	ACEPTAR EL RIESGO	12.6.1 Gestión de vulnerabilidades técnicas.
5.4.17. [A.23] Manipulación de los equipos	2	BAJO	ACEPTAR EL RIESGO	16.1.5 Respuesta a incidentes de seguridad de la información.
5.4.19. [A.25] Robo	1	MUY BAJO	ACEPTAR EL RIESGO	17.1.1 Planificación de la continuidad de la seguridad de la información.

- **[HW] HARDWARE - EQUIPOS INFORMÁTICOS: [HW_SW]**

Tabla H.24. Matriz de tratamiento del riesgo [HW_SW]

[HW] HARDWARE- EQUIPOS INFORMÁTICOS				
[HW_SW]	**Switch TP-LINK**			
AMENAZAS	**RIESGO ACTUAL**		**TRATAMIENTO DEL RIESGO**	**CONTROLES/ SALVAGUARDAS SELECCIONADOS ***
	Rt	**NIVEL**	**NIVEL**	
5.1.1. [N.1] Fuego	2	BAJO	ACEPTAR EL RIESGO	5.1.1 Políticas para la seguridad de la información.
5.1.2. [N.2] Daños por agua	2	BAJO	ACEPTAR EL RIESGO	5.1.2 Revisión de las políticas para la seguridad de la información.
5.2.3. [I.*] Desastres industriales	1	MUY BAJO	ACEPTAR EL RIESGO	6.1.1 Roles y responsabilidades de seguridad de la información.
5.2.6. [I.5] Avería de origen físico o lógico	3	MODERADO	REDUCIR EL RIESGO	8.1.3 Uso aceptable de los activos.
5.2.7. [I.6] Corte del suministro eléctrico	4	ALTO	REDUCIR EL RIESGO	8.3.1 Gestión de medios extraíbles.
5.3.2. [E.2] Errores del administrador	4	ALTO	REDUCIR EL RIESGO	8.3.3 Transferencia de medios físicos.
5.3.15. [E.23] Errores de mantenimiento / actualización de equipos (hardware)	2	BAJO	ACEPTAR EL RIESGO	9.1.1 Política de control de accesos.
5.3.17. [E.25] Pérdida de equipos	2	BAJO	ACEPTAR EL RIESGO	9.4.2 Procedimientos seguros de inicio de sesión.
5.4.4. [A.6] Abuso de privilegios de acceso	1	MUY BAJO	ACEPTAR EL RIESGO	12.4.3 Registros de administración y operación.
5.4.9. [A.11] Acceso no autorizado	2	BAJO	ACEPTAR EL RIESGO	12.6.1 Gestión de vulnerabilidades técnicas.
5.4.17. [A.23] Manipulación de los equipos	2	BAJO	ACEPTAR EL RIESGO	16.1.5 Respuesta a incidentes de seguridad de la información.
5.4.19. [A.25] Robo	1	MUY BAJO	ACEPTAR EL RIESGO	17.1.1 Planificación de la continuidad de la seguridad de la información.

- **[HW] HARDWARE- EQUIPOS INFORMÁTICOS: [HW_MV2]**

Tabla H.25. Matriz de tratamiento del riesgo [HW_MV2]

[HW] HARDWARE- EQUIPOS INFORMÁTICOS				
[HW_MV2]	**Teléfonos móviles**			
AMENAZAS	**RIESGO ACTUAL**		**TRATAMIENTO DEL RIESGO**	**CONTROLES/ SALVAGUARDAS SELECCIONADOS ***
	Rt	**NIVEL**	**NIVEL**	
5.1.1. [N.1] Fuego	2	BAJO	ACEPTAR EL RIESGO	5.1.1 Políticas para la seguridad de la información.
5.1.2. [N.2] Daños por agua	3	MODERADO	REDUCIR EL RIESGO	6.1.1 Roles y responsabilidades de seguridad de la información.
5.2.3. [I.*] Desastres industriales	1	MUY BAJO	ACEPTAR EL RIESGO	6.2.1 Política de dispositivo móvil.
5.2.6. [I.5] Avería de origen físico o lógico	3	MODERADO	REDUCIR EL RIESGO	8.1.4 Devolución de activos.
5.2.7. [I.6] Corte del suministro eléctrico	2	BAJO	ACEPTAR EL RIESGO	8.3.1 Gestión de medios extraíbles.
5.3.1. [E.1] Errores de los usuarios	4	ALTO	REDUCIR EL RIESGO	8.3.3 Transferencia de medios físicos.
5.3.2. [E.2] Errores del administrador	3	MODERADO	REDUCIR EL RIESGO	9.1.1 Política de control de accesos.
5.3.12. [E.19] Fugas de información	5	MUY ALTO	REDUCIR EL RIESGO	9.4.2 Procedimientos seguros de inicio de sesión.
5.3.15. [E.23] Errores de mantenimiento / actualización de equipos (hardware)	3	MODERADO	REDUCIR EL RIESGO	12.2.1 Controles contra un malware.
5.3.17. [E.25] Pérdida de equipos	4	ALTO	REDUCIR EL RIESGO	12.3.1 Copias de seguridad de la información.
5.4.3. [A.5] Suplantación de la identidad del usuario	2	BAJO	ACEPTAR EL RIESGO	12.6.1 Gestión de vulnerabilidades técnicas.
5.4.4. [A.6] Abuso de privilegios de acceso	3	MODERADO	REDUCIR EL RIESGO	13.2.1 Políticas y procedimientos de transferencia de información.
5.4.9. [A.11] Acceso no autorizado	2	BAJO	ACEPTAR EL RIESGO	13.2.3 Mensajería electrónica.
5.4.17. [A.23] Manipulación de los equipos	4	ALTO	REDUCIR EL RIESGO	13.2.4 Acuerdos de confidencialidad o no revelación.
5.4.19. [A.25] Robo	3	MODERADO	REDUCIR EL RIESGO	16.1.5 Respuesta a incidentes de seguridad de la información.

- **[HW] HARDWARE - EQUIPOS INFORMÁTICOS: [HW_PC]**

Tabla H.26. Matriz de tratamiento del riesgo [HW_PC]

[HW] HARDWARE- EQUIPOS INFORMÁTICOS				
[HW_PC]	**Computadoras de escritorio**			
AMENAZAS	**RIESGO ACTUAL**		**TRATAMIENTO DEL RIESGO**	**CONTROLES/ SALVAGUARDAS SELECCIONADOS ***
	Rt	**NIVEL**	**NIVEL**	
5.1.1. [N.1] Fuego	2	BAJO	ACEPTAR EL RIESGO	5.1.1 Políticas para la seguridad de la información.
5.1.2. [N.2] Daños por agua	2	BAJO	ACEPTAR EL RIESGO	6.1.1 Roles y responsabilidades de seguridad de la información.
5.2.3. [I.*] Desastres industriales	1	MUY BAJO	ACEPTAR EL RIESGO	8.1.3 Uso aceptable de los activos.
5.2.6. [I.5] Avería de origen físico o lógico	3	MODERADO	REDUCIR EL RIESGO	8.3.1 Gestión de medios extraíbles.
5.2.7. [I.6] Corte del suministro eléctrico	3	MODERADO	REDUCIR EL RIESGO	8.3.3 Transferencia de medios físicos.
5.3.1. [E.1] Errores de los usuarios	4	ALTO	REDUCIR EL RIESGO	9.1.1 Política de control de accesos.
5.3.2. [E.2] Errores del administrador	3	MODERADO	REDUCIR EL RIESGO	9.1.2 Control de acceso a las redes y servicios asociados.
5.3.15. [E.23] Errores de mantenimiento / actualización de equipos (hardware)	4	ALTO	REDUCIR EL RIESGO	9.4.2 Procedimientos seguros de inicio de sesión.
5.3.17. [E.25] Pérdida de equipos	3	MODERADO	REDUCIR EL RIESGO	12.2.1 Controles contra un malware.
5.4.3. [A.5] Suplantación de la identidad del usuario	2	BAJO	ACEPTAR EL RIESGO	12.3.1 Copias de seguridad de la información.
5.4.4. [A.6] Abuso de privilegios de acceso	2	BAJO	ACEPTAR EL RIESGO	12.6.1 Gestión de vulnerabilidades técnicas.
5.4.9. [A.11] Acceso no autorizado	2	BAJO	ACEPTAR EL RIESGO	13.2.1 Políticas y procedimientos de transferencia de información.
5.4.17. [A.23] Manipulación de los equipos	3	MODERADO	REDUCIR EL RIESGO	13.2.4 Acuerdos de confidencialidad o no revelación.
5.4.19. [A.25] Robo	1	MUY BAJO	ACEPTAR EL RIESGO	16.1.5 Respuesta a incidentes de seguridad de la información.

- **[HW] HARDWARE - EQUIPOS INFORMÁTICOS: [HW_MV1]**

Tabla H.27. Matriz de tratamiento del riesgo [HW_MV1]

[HW] HARDWARE- EQUIPOS INFORMÁTICOS					
[HW_MV1] Computadoras Portátiles					
AMENAZAS	**RIESGO ACTUAL**		**TRATAMIENTO DEL RIESGO**	**CONTROLES/ SALVAGUARDAS SELECCIONADOS ***	
	Rt	**NIVEL**	**NIVEL**		
5.1.1. [N.1] Fuego	2	BAJO	ACEPTAR EL RIESGO	5.1.1	Políticas para la seguridad de la información.
5.1.2. [N.2] Daños por agua	2	BAJO	ACEPTAR EL RIESGO	6.1.1	Roles y responsabilidades de seguridad de la información.
5.2.3. [I.*] Desastres industriales	1	MUY BAJO	ACEPTAR EL RIESGO	6.2.1	Política de dispositivo móvil.
5.2.6. [I.5] Avería de origen físico o lógico	3	MODERADO	REDUCIR EL RIESGO	8.1.3	Uso aceptable de los activos.
5.2.7. [I.6] Corte del suministro eléctrico	3	MODERADO	REDUCIR EL RIESGO	8.3.1	Gestión de medios extraíbles.
5.3.1. [E.1] Errores de los usuarios	4	ALTO	REDUCIR EL RIESGO	8.3.3	Transferencia de medios físicos.
5.3.2. [E.2] Errores del administrador	3	MODERADO	REDUCIR EL RIESGO	9.1.1	Política de control de accesos.
5.3.15. [E.23] Errores de mantenimiento / actualización de equipos (hardware)	4	ALTO	REDUCIR EL RIESGO	9.4.2	Procedimientos seguros de inicio de sesión.
5.3.17. [E.25] Pérdida de equipos	3	MODERADO	REDUCIR EL RIESGO	12.2.1	Controles contra un malware.
5.4.3. [A.5] Suplantación de la identidad del usuario	2	BAJO	ACEPTAR EL RIESGO	12.3.1	Copias de seguridad de la información.
5.4.4. [A.6] Abuso de privilegios de acceso	3	MODERADO	REDUCIR EL RIESGO	12.6.1	Gestión de vulnerabilidades técnicas.
5.4.9. [A.11] Acceso no autorizado	2	BAJO	ACEPTAR EL RIESGO	13.2.1	Políticas y procedimientos de transferencia de información.
5.4.17. [A.23] Manipulación de los equipos	4	ALTO	REDUCIR EL RIESGO	13.2.4	Acuerdos de confidencialidad o no revelación.
5.4.19. [A.25] Robo	4	ALTO	REDUCIR EL RIESGO	16.1.5	Respuesta a incidentes de seguridad de la información.

- **[HW] HARDWARE- EQUIPOS INFORMÁTICOS: [HW_WAP]**

Tabla H.28. Matriz de tratamiento del riesgo [HW_WAP]

[HW] HARDWARE- EQUIPOS INFORMÁTICOS				
[HW_WAP]	**Punto de Acceso**			
AMENAZAS	**RIESGO ACTUAL**		**TRATAMIENTO DEL RIESGO**	**CONTROLES/ SALVAGUARDAS SELECCIONADOS ***
	Rt	**NIVEL**	**NIVEL**	
5.1.1. [N.1] Fuego	2	BAJO	ACEPTAR EL RIESGO	5.1.1 Políticas para la seguridad de la información.
5.1.2. [N.2] Daños por agua	3	MODERADO	REDUCIR EL RIESGO	6.1.1 Roles y responsabilidades de seguridad de la información.
5.2.3. [I.*] Desastres industriales	1	MUY BAJO	ACEPTAR EL RIESGO	8.1.3 Uso aceptable de los activos.
5.2.6. [I.5] Avería de origen físico o lógico	3	MODERADO	REDUCIR EL RIESGO	9.1.1 Política de control de accesos.
5.2.7. [I.6] Corte del suministro eléctrico	4	ALTO	REDUCIR EL RIESGO	9.1.2 Control de acceso a las redes y servicios asociados.
5.4.4. [A.6] Abuso de privilegios de acceso	3	MODERADO	REDUCIR EL RIESGO	12.4.1 Registro de eventos.
5.4.9. [A.11] Acceso no autorizado	2	BAJO	ACEPTAR EL RIESGO	13.1.1 Controles de red.
5.4.17. [A.23] Manipulación de los equipos	3	MODERADO	REDUCIR EL RIESGO	16.1.5 Respuesta a incidentes de seguridad de la información.
5.4.19. [A.25] Robo	2	BAJO	ACEPTAR EL RIESGO	17.1.1 Planificación de la continuidad de la seguridad de la información.

- **[HW] HARDWARE - EQUIPOS INFORMÁTICOS: [HW_PT]**

Tabla H.29. Matriz de tratamiento del riesgo [HW_PT]

[HW] HARDWARE- EQUIPOS INFORMÁTICOS				
[HW_PT]	**Impresoras**			
AMENAZAS	**RIESGO ACTUAL/**		**TRATAMIENTO DEL RIESGO**	**CONTROLES/ SALVAGUARDAS SELECCIONADOS ***
	Rt	**NIVEL**	**NIVEL**	
5.1.1. [N.1] Fuego	1	MUY BAJO	ACEPTAR EL RIESGO	5.1.1 Políticas para la seguridad de la información.
5.1.2. [N.2] Daños por agua	2	BAJO	ACEPTAR EL RIESGO	8.1.3 Uso aceptable de los activos.
5.2.3. [I.*] Desastres industriales	1	MUY BAJO	ACEPTAR EL RIESGO	8.3.1 Gestión de medios extraíbles.
5.2.6. [I.5] Avería de origen físico o lógico	2	BAJO	ACEPTAR EL RIESGO	8.3.3 Transferencia de medios físicos.
5.2.7. [I.6] Corte del suministro eléctrico	1	MUY BAJO	ACEPTAR EL RIESGO	12.4.1 Registro de eventos.
5.4.4. [A.6] Abuso de privilegios de acceso	2	BAJO	ACEPTAR EL RIESGO	12.6.1 Gestión de vulnerabilidades técnicas.
5.4.9. [A.11] Acceso no autorizado	1	MUY BAJO	ACEPTAR EL RIESGO	13.1.1 Controles de red.
5.4.17. [A.23] Manipulación de los equipos	2	BAJO	ACEPTAR EL RIESGO	13.1.2 Seguridad de los servicios de red.
5.4.19. [A.25] Robo	1	MUY BAJO	ACEPTAR EL RIESGO	16.1.5 Respuesta a incidentes de seguridad de la información.

- **REDES DE COMUNICACIONES: [Internet Fibra Óptica]**

Tabla H.30. Matriz de tratamiento del riesgo [Internet Fibra Óptica]

[COM] REDES DE COMUNICACIONES				
Internet Fibra Óptica	**Internet Fibra Óptica**			
AMENAZAS	**RIESGO ACTUAL**		**TRATAMIENTO DEL RIESGO**	**CONTROLES/ SALVAGUARDAS SELECCIONADOS ***
	Rt	**NIVEL**	**NIVEL**	
5.2.9. [I.8] Fallo de servicios de comunicaciones	3	MODERADO	REDUCIR EL RIESGO	5.1.1 Políticas para la seguridad de la información.
5.3.2. [E.2] Errores del administrador	3	MODERADO	REDUCIR EL RIESGO	6.1.1 Roles y responsabilidades de seguridad de la información.
5.3.11. [E.18] Destrucción de información	1	MUY BAJO	ACEPTAR EL RIESGO	8.1.3 Uso aceptable de los activos.
5.3.12. [E.19] Fugas de información	2	BAJO	ACEPTAR EL RIESGO	9.1.1 Política de control de accesos.
5.4.3. [A.5] Suplantación de la identidad del usuario	2	BAJO	ACEPTAR EL RIESGO	9.1.2 Control de acceso a las redes y servicios asociados.
5.4.4. [A.6] Abuso de privilegios de acceso	3	MODERADO	REDUCIR EL RIESGO	12.4.1 Registro de eventos.
5.4.9. [A.11] Acceso no autorizado	3	MODERADO	REDUCIR EL RIESGO	13.1.1 Controles de red.
5.4.10. [A.12] Análisis de tráfico	4	ALTO	REDUCIR EL RIESGO	16.1.5 Respuesta a incidentes de seguridad de la información.
5.4.13. [A.15] Modificación deliberada de la información	1	MUY BAJO	ACEPTAR EL RIESGO	17.1.1 Planificación de la continuidad de la seguridad de la información.
5.4.15. [A.19] Divulgación de información	2	BAJO	ACEPTAR EL RIESGO	
5.4.18. [A.24] Denegación de servicio	3	MODERADO	REDUCIR EL RIESGO	

- **REDES DE COMUNICACIONES: [COM_LAN]**

Tabla H.31. Matriz de tratamiento del riesgo [COM_LAN]

[COM] REDES DE COMUNICACIONES				
[COM_LAN]	**Red Local**			
AMENAZAS	**RIESGO ACTUAL**		**TRATAMIENTO DEL RIESGO**	**CONTROLES/ SALVAGUARDAS SELECCIONADOS ***
	Rt	**NIVEL**	**NIVEL**	
5.2.9. [I.8] Fallo de servicios de comunicaciones	4	ALTO	REDUCIR EL RIESGO	5.1.1 Políticas para la seguridad de la información.
5.3.2. [E.2] Errores del administrador	3	MODERADO	REDUCIR EL RIESGO	6.1.1 Roles y responsabilidades de seguridad de la información.
5.3.11. [E.18] Destrucción de información	1	MUY BAJO	ACEPTAR EL RIESGO	8.1.3 Uso aceptable de los activos.
5.3.12. [E.19] Fugas de información	2	BAJO	ACEPTAR EL RIESGO	9.1.1 Política de control de accesos.
5.4.3. [A.5] Suplantación de la identidad del usuario	2	BAJO	ACEPTAR EL RIESGO	9.1.2 Control de acceso a las redes y servicios asociados.
5.4.4. [A.6] Abuso de privilegios de acceso	2	BAJO	ACEPTAR EL RIESGO	12.4.1 Registro de eventos.
5.4.9. [A.11] Acceso no autorizado	3	MODERADO	REDUCIR EL RIESGO	13.1.1 Controles de red.
5.4.10. [A.12] Análisis de tráfico	3	MODERADO	REDUCIR EL RIESGO	13.1.3 Separación en las redes.
5.4.13. [A.15] Modificación deliberada de la información	2	BAJO	ACEPTAR EL RIESGO	16.1.5 Respuesta a incidentes de seguridad de la información.
5.4.15. [A.19] Divulgación de información	3	MODERADO	REDUCIR EL RIESGO	17.1.1 Planificación de la continuidad de la seguridad de la información.
5.4.18. [A.24] Denegación de servicio	2	BAJO	ACEPTAR EL RIESGO	

- **REDES DE COMUNICACIONES: [COM_MB]**

Tabla H.32. Matriz de tratamiento del riesgo [COM_MB]

[COM] REDES DE COMUNICACIONES				
[COM_MB]	**Telefonía Móvil**			
AMENAZAS	**RIESGO ACTUAL**		**TRATAMIENTO DEL RIESGO**	**CONTROLES/ SALVAGUARDAS SELECCIONADOS ***
	Rt	**NIVEL**	**NIVEL**	
5.2.9. [I.8] Fallo de servicios de comunicaciones	3	MODERADO	REDUCIR EL RIESGO	5.1.1 Políticas para la seguridad de la información.
5.3.2. [E.2] Errores del administrador	3	MODERADO	REDUCIR EL RIESGO	6.1.1 Roles y responsabilidades de seguridad de la información.
5.3.11. [E.18] Destrucción de información	2	BAJO	ACEPTAR EL RIESGO	8.1.3 Uso aceptable de los activos.
5.3.12. [E.19] Fugas de información	5	MUY ALTO	REDUCIR EL RIESGO	9.1.1 Política de control de accesos.
5.4.3. [A.5] Suplantación de la identidad del usuario	1	MUY BAJO	ACEPTAR EL RIESGO	9.1.2 Control de acceso a las redes y servicios asociados.
5.4.4. [A.6] Abuso de privilegios de acceso	2	BAJO	ACEPTAR EL RIESGO	12.4.1 Registro de eventos.
5.4.9. [A.11] Acceso no autorizado	3	MODERADO	REDUCIR EL RIESGO	13.1.1 Controles de red.
5.4.10. [A.12] Análisis de tráfico	2	BAJO	ACEPTAR EL RIESGO	13.2.2 Acuerdos de transferencia de información.
5.4.13. [A.15] Modificación deliberada de la información	1	MUY BAJO	ACEPTAR EL RIESGO	16.1.5 Respuesta a incidentes de seguridad de la información.
5.4.15. [A.19] Divulgación de información	5	MUY ALTO	REDUCIR EL RIESGO	17.1.1 Planificación de la continuidad de la seguridad de la información.
5.4.18. [A.24] Denegación de servicio	2	BAJO	ACEPTAR EL RIESGO	

- **REDES DE COMUNICACIONES: [COM_WF]**

Tabla H.33. Matriz de tratamiento del riesgo [COM_WF]

[COM] REDES DE COMUNICACIONES				
[COM_WF]	**Red Inalámbrica**			
AMENAZAS	**RIESGO ACTUAL**		**TRATAMIENTO DEL RIESGO**	**CONTROLES/ SALVAGUARDAS SELECCIONADOS ***
	Rt	**NIVEL**	**NIVEL**	
5.2.9. [I.8] Fallo de servicios de comunicaciones	3	MODERADO	REDUCIR EL RIESGO	5.1.1 Políticas para la seguridad de la información.
5.3.2. [E.2] Errores del administrador	3	MODERADO	REDUCIR EL RIESGO	6.1.1 Roles y responsabilidades de seguridad de la información.
5.3.11. [E.18] Destrucción de información	2	BAJO	ACEPTAR EL RIESGO	8.1.3 Uso aceptable de los activos.
5.3.12. [E.19] Fugas de información	4	ALTO	REDUCIR EL RIESGO	9.1.1 Política de control de accesos.
5.4.3. [A.5] Suplantación de la identidad del usuario	2	BAJO	ACEPTAR EL RIESGO	9.1.2 Control de acceso a las redes y servicios asociados.
5.4.4. [A.6] Abuso de privilegios de acceso	3	MODERADO	REDUCIR EL RIESGO	12.4.1 Registro de eventos.
5.4.9. [A.11] Acceso no autorizado	3	MODERADO	REDUCIR EL RIESGO	13.1.1 Controles de red.
5.4.10. [A.12] Análisis de tráfico	2	BAJO	ACEPTAR EL RIESGO	16.1.5 Respuesta a incidentes de seguridad de la información.
5.4.13. [A.15] Modificación deliberada de la información	1	MUY BAJO	ACEPTAR EL RIESGO	17.1.1 Planificación de la continuidad de la seguridad de la información.
5.4.15. [A.19] Divulgación de información	3	MODERADO	REDUCIR EL RIESGO	
5.4.18. [A.24] Denegación de servicio	2	BAJO	ACEPTAR EL RIESGO	

- **EQUIPO AUXILIAR: [AUX_CB]**

Tabla H.34. Matriz de tratamiento del riesgo [AUX_CB]

[AUX] EQUIPO AUXILIAR				
[AUX_CB]	**Cableado Estructurado**			
AMENAZAS	**RIESGO ACTUAL**		**TRATAMIENTO DEL RIESGO**	**CONTROLES/ SALVAGUARDAS SELECCIONADOS ***
	Rt	**NIVEL**	**NIVEL**	
5.1.1. [N.1] Fuego	1	MUY BAJO	ACEPTAR EL RIESGO	5.1.1 Políticas para la seguridad de la información.
5.1.2. [N.2] Daños por agua	2	BAJO	ACEPTAR EL RIESGO	6.1.1 Roles y responsabilidades de seguridad de la información.
5.2.3. [I.*] Desastres industriales	1	MUY BAJO	ACEPTAR EL RIESGO	8.1.1 Inventario de activos.
5.2.4. [I.3] Contaminación mecánica	3	MODERADO	REDUCIR EL RIESGO	8.1.3 Uso aceptable de los activos.
5.2.6. [I.5] Avería de origen físico o lógico	2	BAJO	ACEPTAR EL RIESGO	9.1.1 Política de control de accesos.
5.2.7. [I.6] Corte del suministro eléctrico	4	ALTO	REDUCIR EL RIESGO	9.1.2 Control de acceso a las redes y servicios asociados.
5.2.10. [I.9] Interrupción de otros servicios y suministros esenciales	3	MODERADO	REDUCIR EL RIESGO	12.4.1 Registro de eventos.
5.3.15. [E.23] Errores de mantenimiento / actualización de equipos (hardware)	3	MODERADO	REDUCIR EL RIESGO	13.1.1 Controles de red.
5.3.17. [E.25] Pérdida de equipos	3	MODERADO	REDUCIR EL RIESGO	16.1.5 Respuesta a incidentes de seguridad de la información.
5.4.9. [A.11] Acceso no autorizado	2	BAJO	ACEPTAR EL RIESGO	17.1.1 Planificación de la continuidad de la seguridad de la información.
5.4.17. [A.23] Manipulación de los equipos	4	ALTO	REDUCIR EL RIESGO	
5.4.19. [A.25] Robo	1	MUY BAJO	ACEPTAR EL RIESGO	

- **EQUIPO AUXILIAR: [AUX_VIDEO]**

Tabla H.35. Matriz de tratamiento del riesgo [AUX_VIDEO]

[AUX] EQUIPO AUXILIAR				
[AUX_VIDEO]	**Sistema de Video vigilancia**			
AMENAZAS	**RIESGO ACTUAL**		**TRATAMIENTO DEL RIESGO**	**CONTROLES/ SALVAGUARDAS SELECCIONADOS ***
	Rt	**NIVEL**	**NIVEL**	
5.1.1. [N.1] Fuego	1	MUY BAJO	ACEPTAR EL RIESGO	5.1.1 Políticas para la seguridad de la información.
5.1.2. [N.2] Daños por agua	2	BAJO	ACEPTAR EL RIESGO	6.1.1 Roles y responsabilidades de seguridad de la información.
5.2.3. [I.*] Desastres industriales	1	MUY BAJO	ACEPTAR EL RIESGO	8.1.1 Inventario de activos.
5.2.4. [I.3] Contaminación mecánica	3	MODERADO	REDUCIR EL RIESGO	8.1.3 Uso aceptable de los activos.
5.2.6. [I.5] Avería de origen físico o lógico	2	BAJO	ACEPTAR EL RIESGO	9.1.1 Política de control de accesos.
5.2.7. [I.6] Corte del suministro eléctrico	4	ALTO	REDUCIR EL RIESGO	9.1.2 Control de acceso a las redes y servicios asociados.
5.2.10. [I.9] Interrupción de otros servicios y suministros esenciales	3	MODERADO	REDUCIR EL RIESGO	12.4.1 Registro de eventos.
5.3.15. [E.23] Errores de mantenimiento / actualización de equipos (hardware)	3	MODERADO	REDUCIR EL RIESGO	12.5.1 Instalación del software en los sistemas operativos.
5.3.17. [E.25] Pérdida de equipos	2	BAJO	ACEPTAR EL RIESGO	13.1.1 Controles de red.
5.4.9. [A.11] Acceso no autorizado	3	MODERADO	REDUCIR EL RIESGO	16.1.5 Respuesta a incidentes de seguridad de la información.
5.4.17. [A.23] Manipulación de los equipos	3	MODERADO	REDUCIR EL RIESGO	17.1.1 Planificación de la continuidad de la seguridad de la información.
5.4.19. [A.25] Robo	1	MUY BAJO	ACEPTAR EL RIESGO	

- **EQUIPO AUXILIAR: [AUX_UPS]**

Tabla H.36. Matriz de tratamiento del riesgo [AUX_UPS]

[AUX] EQUIPO AUXILIAR				
[AUX_UPS]	**Sistema de alimentación Interrumpida**			
AMENAZAS	**RIESGO ACTUAL**		**TRATAMIENTO DEL RIESGO**	**CONTROLES/ SALVAGUARDAS SELECCIONADOS ***
	Rt	**NIVEL**	**NIVEL**	
5.1.1. [N.1] Fuego	1	MUY BAJO	ACEPTAR EL RIESGO	5.1.1 Políticas para la seguridad de la información.
5.1.2. [N.2] Daños por agua	1	MUY BAJO	ACEPTAR EL RIESGO	8.1.1 Inventario de activos.
5.2.3. [I.*] Desastres industriales	1	MUY BAJO	ACEPTAR EL RIESGO	8.1.3 Uso aceptable de los activos.
5.2.4. [I.3] Contaminación mecánica	2	BAJO	ACEPTAR EL RIESGO	16.1.5 Respuesta a incidentes de seguridad de la información.
5.2.6. [I.5] Avería de origen físico o lógico	1	MUY BAJO	ACEPTAR EL RIESGO	17.1.1 Planificación de la continuidad de la seguridad de la información.
5.2.7. [I.6] Corte del suministro eléctrico	3	MODERADO	REDUCIR EL RIESGO	
5.3.15. [E.23] Errores de mantenimiento / actualización de equipos (hardware)	1	MUY BAJO	ACEPTAR EL RIESGO	
5.3.17. [E.25] Pérdida de equipos	1	MUY BAJO	ACEPTAR EL RIESGO	
5.4.17. [A.23] Manipulación de los equipos	2	BAJO	ACEPTAR EL RIESGO	
5.4.19. [A.25] Robo	1	MUY BAJO	ACEPTAR EL RIESGO	

I. ANEXO I: ANÁLISIS DEL RIESGO PLANIFICADO

- **INFORMACIÓN: [INFO_VR]**

Tabla I.1. Matriz de Gestión de Riesgos Actual y Planificado [INFO_VR]

[INFO] INFORMACIÓN																							
[INFO_VR]	Registros confidenciales de la organización																						
AMENAZAS	RIESGO POTENCIAL					CONTROLES/ SALVAGUARDAS EXISTENTES	NIVEL DE MADUREZ - CONTROLES EXISTENTES		RIESGO ACTUAL					CONTROLES/ SALVAGUARDAS SELECCIONADOS		NIVEL DE MADUREZ - CONTROLES ESTABLECIDOS		RIESGO PLANIFICADO				
	RIESGO POTENCIAL DIMENSIONES			RIESGO POTENCIAL TOTAL					RIESGO POR DIMENSIONES			RIESGO ACTUAL TOTAL						RIESGO POR DIMENSIONES			RIESGO TOTAL	
	Ri	Rc	Rd	Rt	NIVEL		NIVEL	PUNTOS	Ri	Rc	Rd	Rt	NIVEL			NIVEL	PUNTOS	Ri	Rc	Rd	Rt	NIVEL
5.3.1. [E.1] Errores de los usuarios	5	5	5	5	MUY ALTO	No existen controles establecidos para políticas de seguridad de la información bien definidas.	L1	1	4	4	4	4	ALTO	5.1.1	Políticas para la seguridad de la información.	L3	3	1	1	1	1	MUY BAJO
5.3.2. [E.2] Errores del administrador	5	5	5	5	MUY ALTO		L1	1	4	4	4	4	ALTO	6.1.5	Gestión de proyectos de seguridad de la información.	L3	3	1	1	1	1	MUY BAJO
5.3.10. [E.15] Alteración accidental de la información	4	1	1	2	BAJO	Existen controles para la gestión de acceso, donde los usuarios tienen perfiles diferentes según los roles y responsabilidades.	L0	0	4	1	1	2	BAJO	8.2.1	Clasificación de la información.	L2	2	2	1	1	2	BAJO
5.3.11. [E.18] Destrucción de información	2	2	2	2	BAJO		L0	0	2	2	2	2	BAJO	9.1.1	Política de control de accesos.	L2	2	1	1	1	1	MUY BAJO
5.3.12. [E.19] Fugas de información	1	2	1	2	BAJO		L0	0	1	2	1	2	BAJO	13.2.1	Políticas y procedimientos de transferencia de información.	L2	2	1	1	1	1	MUY BAJO
5.4.3. [A.5] Suplantación de la identidad del usuario	3	3	1	3	MODERADO	Existen controles de acuerdos de confidencialidad, para una parte de la información confidencial.	L0	0	3	3	1	3	MODERADO	13.2.4	Acuerdos de confidencialidad o no revelación.	L2	2	1	1	1	1	MUY BAJO
5.4.4. [A.6] Abuso de privilegios de acceso	3	3	3	3	MODERADO		L1	1	2	2	2	2	BAJO	16.1.5	Respuesta a incidentes de seguridad de la información.	L3	3	1	1	1	1	MUY BAJO
5.4.9. [A.11] Acceso no autorizado	3	3	1	3	MODERADO	Existen controles para la gestión de derechos de propiedad intelectual del activo en cuestión, que a su vez refiere a la documentación de fórmulas químicas del cuero	L1	1	2	2	1	2	BAJO	12.1.2	Gestión de cambios.	L3	3	1	1	1	1	MUY BAJO
5.4.13. [A.15] Modificación deliberada de la información	3	2	2	3	MODERADO		L1	1	2	1	1	2	BAJO	17.1.1	Planificación de la continuidad de la seguridad de la información.	L3	3	1	1	1	1	MUY BAJO
5.4.15. [A.19] Divulgación de información	4	4	1	3	MODERADO		L1	1	3	3	1	3	MODERADO	18.1.2	Derechos de propiedad intelectual.	L3	3	1	1	1	1	MUY BAJO

- **INFORMACIÓN: [INFO_PER]**

Tabla I.2. Matriz de Gestión de Riesgos Actual y Planificado: [INFO_PER]

[INFO] INFORMACIÓN																									
[INFO_PER]	Base de datos de clientes y proveedores																								
AMENAZAS	RIESGO POTENCIAL					CONTROLES/ SALVAGUARDAS EXISTENTES	NIVEL DE MADUREZ - CONTROLES EXISTENTES		RIESGO ACTUAL					CONTROLES/ SALVAGUARDAS SELECCIONADOS			NIVEL DE MADUREZ - CONTROLES ESTABLECIDOS		RIESGO PLANIFICADO					
	RIESGO POTENCIAL POR DIMENSIONES			RIESGO POTENCIAL TOTAL					RIESGO POR DIMENSIONES			RIESGO ACTUAL TOTAL							RIESGO POR DIMENSIONES				RIESGO TOTAL	
	Ri	Rc	Rd	Rt	NIVEL		NIVEL	PUNTOS	Ri	Rc	Rd	Rt	NIVEL				NIVEL	PUNTOS	Ri	Rc	Rd	Rt	NIVEL	
5.3.1. [E.1] Errores de los usuarios	4	4	4	4	ALTO	Existen controles para la gestión de acceso, donde los usuarios tienen perfiles diferentes según los roles y responsabilidades. Existen controles de acuerdos de confidencialidad, para una parte de la información confidencial. No existen controles para la destrucción, fugas y alteración de la información .	L1	1	3	3	3	3	MODERADO	5.1.1	Políticas para la seguridad de la información.	L2	2	1	1	1	1	MUY BAJO
5.3.2. [E.2] Errores del administrador	5	5	5	5	MUY ALTO		L1	1	4	4	4	4	ALTO	6.1.1	Roles y responsabilidades de seguridad de la información.	L2	2	2	2	2	2	BAJO
5.3.10. [E.15] Alteración accidental de la información	3	3	3	3	MODERADO		L0	0	3	3	3	3	MODERADO	8.2.1	Clasificación de la información.	L1	1	2	2	2	2	BAJO
5.3.11. [E.18] Destrucción de información	2	3	3	3	MODERADO		L0	0	2	3	3	3	MODERADO	9.1.1	Política de control de accesos.	L1	1	1	2	2	2	BAJO
5.3.12. [E.19] Fugas de información	4	4	4	4	ALTO		L0	0	4	4	4	4	ALTO	13.2.1	Políticas y procedimientos de transferencia de información.	L2	2	2	2	2	2	BAJO
5.4.3. [A.5] Suplantación de la identidad del usuario	3	3	1	3	MODERADO		L0	0	3	3	1	3	MODERADO	13.2.4	Acuerdos de confidencialidad o no revelación.	L2	2	1	1	1	1	MUY BAJO
5.4.4. [A.6] Abuso de privilegios de acceso	2	2	2	2	BAJO		L2	2	1	1	1	1	MUY BAJO	16.1.5	Respuesta a incidentes de seguridad de la información.	L3	3	1	1	1	1	MUY BAJO
5.4.9. [A.11] Acceso no autorizado	3	3	2	3	MODERADO		L1	1	2	2	1	2	BAJO	12.1.2	Gestión de cambios.	L3	3	1	1	1	1	MUY BAJO
5.4.13. [A.15] Modificación deliberada de la información	2	2	1	2	BAJO		L2	2	1	1	1	1	MUY BAJO	17.1.1	Planificación de la continuidad de la seguridad de la información.	L3	3	1	1	1	1	MUY BAJO
5.4.15. [A.19] Divulgación de información	4	4	1	3	MODERADO		L1	1	3	3	1	3	MODERADO	18.1.2	Derechos de propiedad intelectual.	L2	2	1	1	1	1	MUY BAJO

- **INFORMACIÓN: [INFO_PUB]**

Tabla I.3. Matriz de Gestión de Riesgos Actual y Planificado: [INFO_PUB]

[INFO] INFORMACIÓN																							
[INFO_PUB]	Documentación y permisos de funcionamiento																						
AMENAZAS	RIESGO POTENCIAL					CONTROLES/ SALVAGUARDAS EXISTENTES	NIVEL DE MADUREZ - CONTROLES EXISTENTES		RIESGO ACTUAL					CONTROLES/ SALVAGUARDAS SELECCIONADOS		NIVEL DE MADUREZ - CONTROLES ESTABLECIDOS		RIESGO PLANIFICADO				
	RIESGO POTENCIAL POR DIMENSIONES			RIESGO POTENCIAL TOTAL					RIESGO POR DIMENSIONES			RIESGO ACTUAL TOTAL						RIESGO POR DIMENSIONES				RIESGOL TOTAL
	Ri	Rc	Rd	Rt	NIVEL		NIVEL	PUNTOS	Ri	Rc	Rd	Rt	NIVEL			NIVEL	PUNTOS	Ri	Rc	Rd	Rt	NIVEL
5.3.1. [E.1] Errores de los usuarios	4	4	5	5	MUY ALTO	Existen controles para la gestión de acceso, donde los usuarios tienen perfiles diferentes según los roles y responsabilidades. Existen controles referentes a los acuerdos de confidencialidad, para la gestión de información confidencial. Durante la gestión se firman acuerdos de confidencialidad de las partes involucradas. Existen controles para la gestión de derechos de propiedad intelectual del activo en cuestión, que a su vez refiere a la documentación de fórmulas químicas del cuero.	L1	1	3	3	4	4	ALTO	5.1.1	Políticas para la seguridad de la información.	L2	2	1	1	2	2	BAJO
5.3.2. [E.2] Errores del administrador	5	5	5	5	MUY ALTO		L1	1	4	4	4	4	ALTO	6.1.1	Roles y responsabilidades de seguridad de la información.	L2	2	2	2	2	2	BAJO
5.3.10. [E.15] Alteración accidental de la información	4	1	4	3	MODERADO		L0	0	4	1	4	3	MODERADO	8.2.1	Clasificación de la información.	L1	1	3	1	3	3	MODERADO
5.3.11. [E.18] Destrucción de información	2	2	2	2	BAJO		L0	0	2	2	2	2	BAJO	9.1.1	Política de control de accesos.	L1	1	1	1	1	1	MUY BAJO
5.3.12. [E.19] Fugas de información	1	2	2	2	BAJO		L1	1	1	1	1	1	MUY BAJO	13.2.1	Políticas y procedimientos de transferencia de información.	L2	2	1	1	1	1	MUY BAJO
5.4.3. [A.5] Suplantación de la identidad del usuario	2	2	1	2	BAJO		L0	0	2	2	1	2	BAJO	13.2.4	Acuerdos de confidencialidad o no revelación.	L2	2	1	1	1	1	MUY BAJO
5.4.4. [A.6] Abuso de privilegios de acceso	2	2	1	2	BAJO		L2	2	1	1	1	1	MUY BAJO	16.1.5	Respuesta a incidentes de seguridad de la información.	L3	3	1	1	1	1	MUY BAJO
5.4.9. [A.11] Acceso no autorizado	2	2	2	2	BAJO		L1	1	1	1	1	1	MUY BAJO	12.1.2	Gestión de cambios.	L2	2	1	1	1	1	MUY BAJO
5.4.13. [A.15] Modificación deliberada de la información	3	2	2	3	MODERADO		L2	2	1	1	1	1	MUY BAJO	17.1.1	Planificación de la continuidad de la seguridad de la información.	L3	3	1	1	1	1	MUY BAJO
5.4.15. [A.19] Divulgación de información	4	4	4	4	ALTO		L2	2	2	2	2	2	BAJO	18.1.2	Derechos de propiedad intelectual.	L2	2	1	1	1	1	MUY BAJO

- **DATOS E INFORMACIÓN COMPLEMENTARIA: [D_BCK]**

Tabla I.4. Matriz de Gestión de Riesgos Actual y Planificado: [D_BCK]

[DI] DATOS E INFORMACIÓN COMPLEMENTARIA																									
[D_BCK]	Copias de seguridad OwnCloud																								
AMENAZAS	RIESGO POTENCIAL					CONTROLES/ SALVAGUARDAS EXISTENTES	NIVEL DE MADUREZ - CONTROLES EXISTENTES		RIESGO ACTUAL					CONTROLES/ SALVAGUARDAS SELECCIONADOS		NIVEL DE MADUREZ - CONTROLES ESTABLECIDOS		RIESGO PLANIFICADO					
	RIESGO POTENCIAL POR DIMENSIONES			RIESGO POTENCIAL TOTAL					RIESGO POR DIMENSIONES			RIESGO ACTUAL TOTAL					RIESGO POR DIMENSIONES				RIESGO TOTAL	
	Ri	Rc	Rd	Rt	NIVEL		NIVEL	PUNTOS	Ri	Rc	Rd	Rt	NIVEL			NIVEL	PUNTOS	Ri	Rc	Rd	Rt	NIVEL	
5.3.1. [E.1] Errores de los usuarios	2	2	2	2	BAJO	Existen controles para la gestión de acceso, donde los usuarios tienen perfiles diferentes según los roles y responsabilidades. Existen controles referentes a los acuerdos de confidencialidad, para la gestión de información confidencial. Durante la gestión se firman acuerdos de confidencialidad de las partes involucradas. No existen controles para la gestión de las copias de seguridad de la información.	L1	1	1	1	1	1	MUY BAJO	5.1.1	Políticas para la seguridad de la información.	L2	2	1	1	1	1	MUY BAJO
5.3.2. [E.2] Errores del administrador	4	4	4	4	ALTO		L1	1	3	3	3	3	MODERADO	6.1.1	Roles y responsabilidades de seguridad de la información.	L2	2	1	1	1	1	MUY BAJO
5.3.10. [E.15] Alteración accidental de la información	3	3	2	3	MODERADO		L1	1	2	2	1	3	MODERADO	8.1.3	Uso aceptable de los activos.	L1	1	1	1	1	1	MUY BAJO
5.3.11. [E.18] Destrucción información	1	2	2	2	BAJO		L0	0	1	2	2	2	BAJO	8.2.1	Clasificación de la información.	L1	1	1	1	1	1	MUY BAJO
5.3.12. [E.19] Fugas de información	2	2	1	2	BAJO		L1	1	1	1	1	1	MUY BAJO	8.3.1	Gestión de medios extraíbles.	L2	2	1	1	1	1	MUY BAJO
5.4.3. [A.5] Suplantación de la identidad del usuario	3	3	2	3	MODERADO		L0	0	3	3	2	3	MODERADO	9.1.1	Política de control de accesos.	L2	2	1	1	1	1	MUY BAJO
5.4.4. [A.6] Abuso de privilegios de acceso	3	3	3	3	MODERADO		L2	2	1	1	1	1	MUY BAJO	9.4.1	Restricción del acceso a la información.	L3	3	1	1	1	1	MUY BAJO
5.4.9. [A.11] Acceso no autorizado	3	3	3	3	MODERADO		L1	1	2	2	2	2	BAJO	12.3.1	Copias de seguridad de la información.	L2	2	1	1	1	1	MUY BAJO
5.4.13. [A.15] Modificación deliberada de la información	3	2	2	3	MODERADO		L2	2	1	1	1	1	MUY BAJO	12.1.2	Gestión de cambios.	L3	3	1	1	1	1	MUY BAJO
5.4.15. [A.19] Divulgación información	3	4	4	4	ALTO		L2	2	1	2	2	2	BAJO	13.2.4	Acuerdos de confidencialidad o no revelación.	L2	2	1	1	1	1	MUY BAJO

- **DATOS E INFORMACIÓN COMPLEMENTARIA: [D_LG]**

Tabla I.5. Matriz de Gestión de Riesgos Actual y Planificado: [D_LG]

[DI] DATOS E INFORMACIÓN COMPLEMENTARIA																									
[D_LG]	Logs de SACI																								
AMENAZAS	RIESGO POTENCIAL					CONTROLES/ SALVAGUARDAS EXISTENTES	NIVEL DE MADUREZ - CONTROLES EXISTENTES		RIESGO ACTUAL					CONTROLES/ SALVAGUARDAS SELECCIONADOS		NIVEL DE MADUREZ - CONTROLES ESTABLECIDOS		RIESGO PLANIFICADO					
	RIESGO POTENCIAL DIMENSIONES			RIESGO POTENCIAL TOTAL					RIESGO POR DIMENSIONES			RIESGO ACTUAL TOTAL						RIESGO POR DIMENSIONES				RIESGO TOTAL	
	Ri	Rc	Rd	Rt	NIVEL		NIVEL	PUNTOS	Ri	Rc	Rd	Rt	NIVEL			NIVEL	PUNTOS	Ri	Rc	Rd	Rt	NIVEL	
5.3.1. [E.1] Errores de los usuarios	3	3	3	3	MODERADO	Existen controles para la gestión de acceso, donde los usuarios tienen perfiles diferentes según los roles y responsabilidades. Existen controles referentes a los acuerdos de confidencialidad, para la gestión de información confidencial. Durante la gestión se firman acuerdos de confidencialidad de las partes involucradas. Existen controles para la gestión de derechos de propiedad intelectual del activo en cuestión, que a su vez refiere a la documentación de fórmulas químicas del cuero. No existen controles para la gestión de los logs del sistema contable SACI.	L0	0	3	3	3	3	MODERADO	5.1.1	Políticas para la seguridad de la información.	L1	1	2	2	2	2	BAJO
5.3.2. [E.2] Errores del administrador	4	4	4	4	ALTO		L1	1	3	3	3	3	MODERADO	6.1.1	Roles y responsabilidades de seguridad de la información.	L2	2	1	1	2	2	BAJO
5.3.3. [E.3] Errores de monitorización	4	4	2	4	ALTO		L1	1	3	3	1	3	MODERADO	8.1.3	Uso aceptable de los activos.	L1	1	2	2	1	2	BAJO
5.3.10. [E.15] Alteración accidental de la información	3	3	2	3	MODERADO		L0	0	3	3	2	3	MODERADO	8.2.1	Clasificación de la información.	L1	1	2	2	1	2	BAJO
5.3.11. [E.18] Destrucción de información	1	2	2	2	BAJO		L1	1	1	1	1	1	MUY BAJO	8.2.2	Etiquetado de la información.	L2	2	1	1	1	1	MUY BAJO
5.3.12. [E.19] Fugas de información	4	4	3	4	ALTO		L1	1	3	3	2	3	MODERADO	9.1.1	Política de control de accesos.	L2	2	1	1	1	1	MUY BAJO
5.4.1. [A.3] Manipulación de los registros de actividad	2	2	2	2	BAJO		L0	0	1	1	1	1	MUY BAJO	9.1.2	Control de acceso a las redes y servicios asociados.	L3	3	1	1	1	1	MUY BAJO
5.4.3. [A.5] Suplantación de la identidad del usuario	3	3	2	3	MODERADO		L1	1	2	2	1	2	BAJO	9.2.3	Gestión de privilegios de derechos de acceso.	L2	2	1	1	1	1	MUY BAJO
5.4.4. [A.6] Abuso de privilegios de acceso	3	3	3	3	MODERADO		L2	2	1	1	1	1	MUY BAJO	12.1.2	Gestión de cambios.	L3	3	1	1	1	1	MUY BAJO
5.4.9. [A.11] Acceso no autorizado	2	2	1	2	BAJO		L1	1	1	1	1	1	MUY BAJO	12.3.1	Copias de seguridad de la información.	L3	3	1	1	1	1	MUY BAJO
5.4.13. [A.15] Modificación deliberada de la información	3	2	2	3	MODERADO		L2	2	1	1	1	1	MUY BAJO	16.1.7	Recopilación de evidencias.	L3	3	1	1	1	1	MUY BAJO
5.4.15. [A.19] Divulgación de información	3	4	3	4	ALTO		L2	2	1	1	1	1	MUY BAJO	17.2.1	Disponibilidad de las instalaciones de procesamiento de la información.	L3	3	1	1	1	1	MUY BAJO

- **CLAVES CRIPTOGRÁFICAS: [K_PB]**

Tabla I.6. Matriz de Gestión de Riesgos Actual y Planificado: [K_PB]

[K] CLAVES CRIPTOGRÁFICAS																									
[K_PB]	SSL																								
AMENAZAS	RIESGO POTENCIAL					CONTROLES/ SALVAGUARDAS EXISTENTES	NIVEL DE MADUREZ - CONTROLES EXISTENTES		RIESGO ACTUAL					CONTROLES/ SALVAGUARDAS SELECCIONADOS		NIVEL DE MADUREZ - CONTROLES ESTABLECIDOS		RIESGO PLANIFICADO					
	RIESGO POTENCIAL POR DIMENSIONES			RIESGO POTENCIAL TOTAL					RIESGO POR DIMENSIONES			RIESGO ACTUAL TOTAL					RIESGO POR DIMENSIONES				RIESGO TOTAL	
	Ri	Rc	Rd	Rt	NIVEL		NIVEL	PUNTOS	Ri	Rc	Rd	Rt	NIVEL			NIVEL	PUNTOS	Ri	Rc	Rd	Rt	NIVEL	
5.3.1. [E.1] Errores de los usuarios	2	2	2	2	BAJO	Existen controles para la gestión de acceso, donde los usuarios tienen perfiles diferentes según los roles y responsabilidades. No existen controles que permitan la gestión de llaves criptográficas. Existen procedimientos que permiten la gestión de vulnerabilidades del certificado SSL.	L0	0	2	2	2	2	BAJO	5.1.1	Políticas para la seguridad de la información.	L1	1	1	1	1	1	MUY BAJO
5.3.2. [E.2] Errores del administrador	4	4	4	4	ALTO		L1	1	3	3	3	3	MODERADO	6.1.4	Contacto con grupos de interés especial.	L2	2	1	1	1	1	MUY BAJO
5.3.10. [E.15] Alteración accidental de la información	3	2	1	2	BAJO		L1	1	2	1	0	3	MODERADO	9.2.3	Gestión de privilegios de derechos de acceso.	L1	1	1	1	1	1	MUY BAJO
5.3.11. [E.18] Destrucción de información	1	1	2	2	BAJO		L0	0	1	1	2	3	MODERADO	9.4.2	Procedimientos seguros de inicio de sesión.	L1	1	1	1	1	1	MUY BAJO
5.3.12. [E.19] Fugas de información	1	3	2	2	BAJO		L1	1	1	2	1	1	MUY BAJO	10.1.1	Política de uso de los controles criptográficos.	L2	2	1	1	1	1	MUY BAJO
5.4.3. [A.5] Suplantación de la identidad del usuario	2	2	2	2	BAJO		L1	1	1	1	1	3	MODERADO	10.1.2	Gestión de Llaves.	L2	2	1	1	1	1	MUY BAJO
5.4.4. [A.6] Abuso de privilegios de acceso	2	2	2	2	BAJO		L0	0	1	1	1	1	MUY BAJO	12.3.1	Copias de seguridad de la información.	L3	3	1	1	1	1	MUY BAJO
5.4.9. [A.11] Acceso no autorizado	3	3	3	3	MODERADO		L1	1	2	2	2	2	BAJO	12.6.1	Gestión de vulnerabilidades técnicas.	L2	2	1	1	1	1	MUY BAJO
5.4.13. [A.15] Modificación deliberada de la información	2	2	2	2	BAJO		L2	2	1	1	1	1	MUY BAJO	13.1.2	Seguridad de los servicios de red.	L3	3	1	1	1	1	MUY BAJO
5.4.15. [A.19] Divulgación de información	1	2	1	2	BAJO		L1	1	1	1	1	1	MUY BAJO	13.2.4	Acuerdos de confidencialidad o no revelación.	L3	3	1	1	1	1	MUY BAJO

- **CLAVES CRIPTOGRÁFICAS: [K_SIGN]**

Tabla I.7. Matriz de Gestión de Riesgos Actual y Planificado: [K_SIGN]

[K] CLAVES CRIPTOGRÁFICAS																									
[K_SIGN]	Token Digital																								
AMENAZAS	RIESGO POTENCIAL					CONTROLES/ SALVAGUARDAS	NIVEL DE MADUREZ - CONTROLES EXISTENTES		RIESGO ACTUAL					CONTROLES/ SALVAGUARDAS		NIVEL DE MADUREZ - CONTROLES ESTABLECIDOS		RIESGO PLANIFICADO					
	RIESGO POTENCIAL POR DIMENSIONES			RIESGO POTENCIAL TOTAL					RIESGO POR DIMENSIONES			RIESGO ACTUAL TOTAL						RIESGO POR DIMENSIONES				RIESGO TOTAL	
	Ri	Rc	Rd	Rt	NIVEL		NIVEL	PUNTOS	Ri	Rc	Rd	Rt	NIVEL			NIVEL	PUNTOS	Ri	Rc	Rd	Rt	NIVEL	
5.3.1. [E.1] Errores de los usuarios	2	3	2	3	MODERADO	Existen controles para la gestión de acceso, donde los usuarios tienen perfiles diferentes según los roles y responsabilidades.	L0	0	2	3	2	3	MODERADO	5.1.1	Políticas para la seguridad de la información.	L1	1	1	2	1	2	BAJO
5.3.2. [E.2] Errores del administrador	4	4	4	4	ALTO		L1	1	3	3	3	3	MODERADO	8.3.1	Gestión de medios extraíbles.	L2	2	1	1	1	1	MUY BAJO
5.3.10. [E.15] Alteración accidental de la información	4	4	4	4	ALTO		L1	1	3	3	3	3	MODERADO	8.3.2	Eliminación de los medios.	L1	1	2	2	2	2	BAJO
5.3.11. [E.18] Destrucción de información	2	2	2	2	BAJO	Existen controles referentes a los acuerdos de confidencialidad, para la gestión de información confidencial. Durante la gestión se firman acuerdos de confidencialidad de las partes involucradas.	L0	0	2	2	2	2	BAJO	9.3.1	Uso de la información secreta de autenticación.	L1	1	1	1	1	1	MUY BAJO
5.3.12. [E.19] Fugas de información	2	2	2	2	BAJO		L1	1	1	1	1	1	MUY BAJO	10.1.1	Política de uso de los controles criptográficos.	L2	2	1	1	1	1	MUY BAJO
5.4.3. [A.5] Suplantación de la identidad del usuario	3	3	3	3	MODERADO		L1	1	2	2	2	3	MODERADO	10.1.2	Gestión de Llaves.	L2	2	1	1	1	1	MUY BAJO
5.4.4. [A.6] Abuso de privilegios de acceso	2	2	2	2	BAJO		L0	0	1	1	1	1	MUY BAJO	12.3.1	Copias de seguridad de la información.	L3	3	1	1	1	1	MUY BAJO
5.4.9. [A.11] Acceso no autorizado	3	3	2	3	MODERADO	Existe un control que permite la gestión de llaves, a través de un procedimiento empírico.	L1	1	2	2	1	2	BAJO	12.6.1	Gestión de vulnerabilidades técnicas.	L2	2	1	1	1	1	MUY BAJO
5.4.13. [A.15] Modificación deliberada de la información	2	2	2	2	BAJO		L2	2	1	1	1	1	MUY BAJO	13.1.2	Seguridad de los servicios de red.	L3	3	1	1	1	1	MUY BAJO
5.4.15. [A.19] Divulgación de información	2	2	2	2	BAJO		L1	1	1	1	1	1	MUY BAJO	13.2.4	Acuerdos de confidencialidad o no revelación.	L3	3	1	1	1	1	MUY BAJO

- **SERVICIOS [S_INT]**

Tabla I.8. Matriz de Gestión de Riesgos Actual y Planificado: [S_INT]

[S] SERVICIOS																									
[S_INT]	Servicio del sistema contable																								
AMENAZAS	RIESGO POTENCIAL					CONTROLES/ SALVAGUARDAS EXISTENTES	NIVEL DE MADUREZ - CONTROLES EXISTENTES		RIESGO ACTUAL					CONTROLES/ SALVAGUARDAS SELECCIONADOS			NIVEL DE MADUREZ - CONTROLES ESTABLECIDOS		RIESGO PLANIFICADO					
	RIESGO POTENCIAL POR DIMENSIONES			RIESGO POTENCIAL TOTAL					RIESGO POR DIMENSIONES			RIESGO ACTUAL TOTAL						RIESGO POR DIMENSIONES			RIESGO TOTAL		
	Ri	Rc	Rd	Rt	NIVEL		NIVEL	PUNTOS	Ri	Rc	Rd	Rt	NIVEL				NIVEL	PUNTOS	Ri	Rc	Rd	Rt	NIVEL	
5.3.1. [E.1] Errores de los usuarios	5	5	4	5	MUY ALTO	Existen controles para la gestión de acceso, donde los usuarios tienen perfiles diferentes según los roles y responsabilidades. Existen controles referentes a los acuerdos de confidencialidad, para la gestión de información confidencial. Durante la gestión se firman acuerdos de confidencialidad de las partes involucradas. Existe un control que permite el contacto directo con grupos de interés especial en el tema.	L1	1	4	4	3	4	ALTO	5.1.1	Políticas para la seguridad de la información.	L2	2	2	2	1	2	BAJO
5.3.2. [E.2] Errores del administrador	5	5	5	5	MUY ALTO		L1	1	4	4	4	4	ALTO	6.1.2	Separación de funciones.	L2	2	2	2	2	2	BAJO
5.3.10. [E.15] Alteración accidental de la información	4	3	1	3	MODERADO		L1	1	3	2	1	3	MODERADO	6.1.4	Contacto con grupos de interés especial.	L2	2	1	1	1	1	MUY BAJO
5.3.11. [E.18] Destrucción de información	1	2	2	2	BAJO		L0	0	1	2	2	2	BAJO	9.2.2	Provisión de accesos a usuarios.	L1	1	1	1	1	1	MUY BAJO
5.3.12. [E.19] Fugas de información	1	4	2	3	MODERADO		L1	1	1	3	1	1	MUY BAJO	9.2.1	Registro y retiro de usuario.	L2	2	1	1	1	1	MUY BAJO
5.4.3. [A.5] Suplantación de la identidad del usuario	4	4	3	4	ALTO		L1	1	3	3	2	3	MODERADO	9.2.3	Gestión de privilegios de derechos de acceso.	L2	2	1	1	1	1	MUY BAJO
5.4.4. [A.6] Abuso de privilegios de acceso	2	2	2	2	BAJO		L0	0	2	2	2	1	MUY BAJO	9.2.4	Gestión de la información secreta de autenticación de los usuarios.	L3	3	1	1	1	1	MUY BAJO
5.4.9. [A.11] Acceso no autorizado	3	3	1	3	MODERADO		L1	1	2	2	1	2	BAJO	13.1.2	Seguridad de los servicios de red.	L2	2	1	1	1	1	MUY BAJO
5.4.13. [A.15] Modificación deliberada de la información	2	2	1	2	BAJO		L2	2	1	1	1	1	MUY BAJO	16.1.1	Responsabilidades y procedimientos.	L3	3	1	1	1	1	MUY BAJO
5.4.15. [A.19] Divulgación de información	2	4	2	3	MODERADO		L1	1	1	3	1	1	MUY BAJO	16.1.5	Respuesta a incidentes de seguridad de la información.	L3	3	1	1	1	1	MUY BAJO

- **SERVICIOS [S_WWW]**

Tabla I.9. Matriz de Gestión de Riesgos Actual y Planificado: [S_WWW]

[S] SERVICIOS																									
[S_WWW]	Sitio web																								
AMENAZAS	RIESGO POTENCIAL					CONTROLES/ SALVAGUARDAS EXISTENTES	NIVEL DE MADUREZ - CONTROLES EXISTENTES		RIESGO ACTUAL					CONTROLES/ SALVAGUARDAS SELECCIONADOS			NIVEL DE MADUREZ - CONTROLES ESTABLECIDOS		RIESGO PLANIFICADO					
	RIESGO POTENCIAL DIMENSIONES			RIESGO POTENCIAL TOTAL					RIESGO POR DIMENSIONES			RIESGO ACTUAL TOTAL							RIESGO POR DIMENSIONES				RIESGO TOTAL	
	Ri	Rc	Rd	Rt	NIVEL		NIVEL	PUNTOS	Ri	Rc	Rd	Rt	NIVEL			NIVEL	PUNTOS	Ri	Rc	Rd	Rt	NIVEL		
5.3.1. [E.1] Errores de los usuarios	4	4	4	4	ALTO	Existen controles para la gestión de acceso, donde los usuarios tienen perfiles diferentes según los roles y responsabilidades. No existen controles que permitan la gestión de acceso a redes y servicios asociados. No existe un control que permita la gestión de contraseñas. Existen controles que permiten la gestión de la seguridad de los servicios de red.	L0	0	4	4	4	4	ALTO	5.1.1	Políticas para la seguridad de la información.	L2	2	2	2	2	2	BAJO
5.3.2. [E.2] Errores del administrador	4	4	4	4	ALTO		L1	1	3	3	3	3	MODERADO	6.1.4	Contacto con grupos de interés especial.	L2	2	1	1	1	1	MUY BAJO		
5.3.10. [E.15] Alteración accidental de la información	4	4	3	4	ALTO		L0	0	4	4	3	4	ALTO	9.1.1	Política de control de accesos.	L1	1	3	3	2	2	BAJO		
5.3.11. [E.18] Destrucción información	1	2	2	2	BAJO		L0	0	1	2	2	2	BAJO	9.1.2	Control de acceso a las redes y servicios asociados.	L1	1	0	1	1	1	MUY BAJO		
5.3.12. [E.19] Fugas de información	2	4	4	4	ALTO		L0	0	2	4	4	4	ALTO	9.2.5	Revisión de los derechos de acceso de usuario.	L2	2	1	2	2	2	BAJO		
5.4.3. [A.5] Suplantación de la identidad del usuario	4	4	4	4	ALTO		L0	0	4	4	4	4	ALTO	9.2.6	Retiro y ajuste de los derechos de acceso.	L1	1	3	3	3	3	MODERADO		
5.4.4. [A.6] Abuso de privilegios de acceso	2	2	2	2	BAJO		L0	0	2	2	2	2	BAJO	9.4.2	Procedimientos seguros de inicio de sesión.	L2	2	1	1	1	1	MUY BAJO		
5.4.9. [A.11] Acceso no autorizado	3	3	2	3	MODERADO		L1	1	2	2	1	2	BAJO	9.4.3	Sistema de gestión de contraseñas.	L2	2	1	1	1	1	MUY BAJO		
5.4.13. [A.15] Modificación deliberada de la información	2	2	1	2	BAJO		L2	2	1	1	1	1	MUY BAJO	12.4.2	Protección de la información de registro.	L3	3	1	1	1	1	MUY BAJO		
5.4.15. [A.19] Divulgación información	2	4	1	3	MODERADO		L0	0	2	4	1	2	BAJO	13.1.2	Seguridad de los servicios de red.	L1	1	1	3	1	2	BAJO		
5.4.18. [A.24] Denegación de servicio	1	2	2	2	BAJO		L0	0	1	2	2	2	BAJO	16.1.5	Respuesta a incidentes de seguridad de la información.	L1	1	1	1	1	1	MUY BAJO		

- **SOFTWARE- APLICACIONES INFORMÁTICAS: [SW_HP]**

Tabla I.10. Matriz de Gestión de Riesgos Actual y Planificado: [SW_HP] (1/2)

[SW] SOFTWARE- APLICACIONES INFORMÁTICAS																									
[SW_HP]	Proxmox																								
AMENAZAS	RIESGO POTENCIAL					CONTROLES/ SALVAGUARDAS EXISTENTES	NIVEL DE MADUREZ - CONTROLES EXISTENTES		RIESGO ACTUAL					CONTROLES/ SALVAGUARDAS SELECCIONADOS		NIVEL DE MADUREZ - CONTROLES ESTABLECIDOS		RIESGO PLANIFICADO					
	RIESGO POTENCIAL DIMENSIONES			RIESGO POTENCIAL TOTAL					RIESGO POR DIMENSIONES			RIESGO ACTUAL TOTAL						RIESGO POR DIMENSIONES			RIESGO TOTAL		
	Ri	Rc	Rd	Rt	NIVEL		NIVEL	PUNTOS	Ri	Rc	Rd	Rt	NIVEL			NIVEL	PUNTOS	Ri	Rc	Rd	Rt	NIVEL		
5.2.6. [I.5] Avería de físico o lógico	1	4	5	4	ALTO	Existen controles para la gestión de acceso, donde los usuarios tienen perfiles diferentes según los roles y responsabilidades. Existen controles referentes a los acuerdos de confidencialidad, para la gestión de información confidencial. Durante la gestión se firman acuerdos de confidencialidad de las partes involucradas.	L0	0	1	4	5	4	ALTO	5.1.1	Políticas para la seguridad de la información.	L2	2	1	2	3	2	BAJO
5.3.1. [E.1] Errores de los usuarios	3	3	3	3	MODERADO		L1	1	2	2	2	3	MODERADO	6.1.4	Contacto con grupos de interés especial.	L2	2	1	1	1	1	MUY BAJO
5.3.2. [E.2] Errores del administrador	2	2	2	2	BAJO		L0	0	2	2	2	4	ALTO	9.4.2	Procedimientos seguros de inicio de sesión.	L1	1	1	1	1	2	BAJO
5.3.6. [E.8] Difusión de software dañino	3	3	3	3	MODERADO		L0	0	3	3	3	2	BAJO	12.1.1	Documentación de procedimientos de operación.	L1	1	2	2	2	1	MUY BAJO
5.3.10. [E.15] Alteración accidental de la información	2	2	2	2	BAJO		L0	0	2	2	2	4	ALTO	12.2.1	Controles contra un malware.	L2	2	1	1	1	2	BAJO
5.3.11. [E.18] Destrucción de información	2	2	2	2	BAJO		L0	0	2	2	2	4	ALTO	12.4.3	Registros de administración y operación.	L1	1	1	1	1	3	MODERADO
5.3.12. [E.19] Fugas de información	2	3	3	3	MODERADO		L0	0	2	3	3	2	BAJO	12.4.4	Sincronización del reloj.	L2	2	1	1	1	1	MUY BAJO
5.3.13. [E.20] Vulnerabilidades de los programas	5	5	5	5	MUY ALTO		L1	1	4	4	4	2	BAJO	12.6.1	Gestión de vulnerabilidades técnicas.	L2	2	2	2	2	1	MUY BAJO
5.3.14. [E.21] Errores de mantenimiento / actualización de programas	5	3	5	5	MUY ALTO		L1	1	1	1	1	1	MUY BAJO	13.1.2	Seguridad de los servicios de red.	L3	3	1	1	1	1	MUY BAJO
5.4.3. [A.5] Suplantación de la identidad del usuario	2	2	2	2	BAJO		L0	0	2	2	2	2	BAJO	13.2.1	Políticas y procedimientos de transferencia de información.	L1	1	1	1	1	2	BAJO

- **SOFTWARE- APLICACIONES INFORMÁTICAS: [SW_HP]**

Tabla I.11. Matriz de Gestión de Riesgos Actual y Planificado: [SW_HP] (2/2)

[SW] SOFTWARE- APLICACIONES INFORMÁTICAS																							
[SW_HP]	Proxmox																						
AMENAZAS	RIESGO POTENCIAL					CONTROLES/ SALVAGUARDAS EXISTENTES	NIVEL DE MADUREZ - CONTROLES EXISTENTES		RIESGO ACTUAL					CONTROLES/ SALVAGUARDAS SELECCIONADOS		NIVEL DE MADUREZ - CONTROLES ESTABLECIDOS		RIESGO PLANIFICADO				
	RIESGO POTENCIAL DIMENSIONES			RIESGO POTENCIAL TOTAL					RIESGO POR DIMENSIONES			RIESGO ACTUAL TOTAL						RIESGO POR DIMENSIONES			RIESGO TOTAL	
	Ri	Rc	Rd	Rt	NIVEL		NIVEL	PUNTOS	Ri	Rc	Rd	Rt	NIVEL			NIVEL	PUNTOS	Ri	Rc	Rd	Rt	NIVEL
5.4.4. [A.6] Abuso de privilegios de acceso	4	4	4	4	ALTO	Existen controles que permiten la gestión de la seguridad de los servicios de red.	L0	0	4	4	4	2	BAJO	13.2.4	Acuerdos de confidencialidad o no revelación.	L1	1	3	3	3	1	MUY BAJO
5.4.9. [A.11] Acceso no autorizado	3	3	2	3	MODERADO		L1	1	1	1	1	1	MUY BAJO	13.2.4	Acuerdos de confidencialidad o no revelación.	L3	3	1	1	1	1	MUY BAJO
						Existe un control que permite la respuesta ante incidentes de seguridad en caso de caída de la plataforma.																	
5.4.13. [A.15] Modificación deliberada de la información	3	3	2	3	MODERADO		L0	0	3	3	2	2	BAJO	16.1.3	Informe de debilidades de seguridad de la información.	L1	1	2	2	1	2	BAJO
5.4.15. [A.19] Divulgación de información	1	3	2	2	BAJO	No existe planificación de continuidad de seguridad de la información	L0	0	1	3	2	2	BAJO	16.1.4	Apreciación y decisión sobre los eventos de seguridad de la información.	L1	1	1	2	1	1	MUY BAJO
5.4.16. [A.22] Manipulación de programas	4	4	4	4	ALTO		L1	1	3	3	3	2	BAJO	16.1.5	Respuesta a incidentes de seguridad de la información.	L1	1	2	2	2	2	BAJO
5.4.18. [A.24] Denegación de servicio	1	2	2	2	BAJO		L0	0	1	2	2	2	BAJO	17.1.1	Planificación de la continuidad de la seguridad de la información.	L1	1	1	1	1	1	MUY BAJO

- **SOFTWARE- APLICACIONES INFORMÁTICAS: [SW_BD1]**

Tabla I.12. Matriz de Gestión de Riesgos Actual y Planificado: [SW_BD1]

[SW] SOFTWARE- APLICACIONES INFORMÁTICAS																									
[SW_BD1]	Servidor de Base de Datos Oracle XE 18c																								
AMENAZAS	RIESGO POTENCIAL					CONTROLES/ SALVAGUARDAS EXISTENTES	NIVEL DE MADUREZ - CONTROLES EXISTENTES		RIESGO ACTUAL					CONTROLES/ SALVAGUARDAS SELECCIONADOS		NIVEL DE MADUREZ - CONTROLES ESTABLECIDOS		RIESGO PLANIFICADO					
	RIESGO POTENCIAL DIMENSIONES			RIESGO POTENCIAL TOTAL					RIESGO POR DIMENSIONES			RIESGO ACTUAL TOTAL						RIESGO POR DIMENSIONES		RIESGO TOTAL				
	Ri	Rc	Rd	Rt	NIVEL		NIVEL	PUNTOS	Ri	Rc	Rd	Rt	NIVEL			NIVEL	PUNTOS	Ri	Rc	Rd	Rt	NIVEL		
5.2.6. [I.5] Avería de origen físico o lógico	2	2	2	2	BAJO	Existen controles para la gestión de acceso, donde los usuarios tienen perfiles diferentes según los roles y responsabilidades.	L0	0	2	2	2	2	BAJO	5.1.1	Políticas para la seguridad de la información.	L1	1	1	1	1	1	MUY BAJO	
5.3.1. [E.1] Errores de los usuarios	4	4	4	4	ALTO		L1	1	3	3	3	3	MODERADO	6.1.1	Roles y responsabilidades de seguridad de la información.	L2	2	1	1	1	1	MUY BAJO	
5.3.2. [E.2] Errores del administrador	4	4	4	4	ALTO		L1	1	3	3	3	3	MODERADO	6.1.4	Contacto con grupos de interés especial.	L2	2	1	1	1	1	MUY BAJO	
5.3.6. [E.8] Difusión de software dañino	3	3	3	3	MODERADO	Existen controles referentes a los acuerdos de confidencialidad, para la gestión de información confidencial. Durante la gestión se firman acuerdos de confidencialidad de las partes involucradas.	L0	0	3	3	3	3	MODERADO	8.2.1	Clasificación de la información.	L1	1	2	2	2	2	BAJO	
5.3.10. [E.15] Alteración accidental de la información	2	2	2	2	BAJO		L0	0	2	2	2	2	BAJO	9.1.1	Política de control de accesos.	L2	2	1	1	1	1	MUY BAJO	
5.3.11. [E.18] Destrucción de información	1	2	2	2	BAJO		L0	0	1	2	2	2	BAJO	9.4.2	Procedimientos seguros de inicio de sesión.	L1	1	1	1	1	1	MUY BAJO	
5.3.12. [E.19] Fugas de información	2	3	2	3	MODERADO	Existe un control que permite la gestión de registros de administración y operación de las bases de datos.	L1	1	1	2	1	2	BAJO	12.1.4	Separación de ambientes de desarrollo, pruebas y producción.	L2	2	1	1	1	1	MUY BAJO	
5.4.3. [A.5] Suplantación de la identidad del usuario	2	2	2	2	BAJO		L1	1	1	1	1	1	MUY BAJO	12.3.1	Copias de seguridad de la información.	L2	2	1	1	1	1	MUY BAJO	
5.4.9. [A.11] Acceso no autorizado	2	2	1	2	BAJO		L1	1	1	1	1	1	MUY BAJO	12.4.3	Registros de administración y operación.	L3	3	1	1	1	1	MUY BAJO	
5.4.13. [A.15] Modificación deliberada de la información	3	3	2	3	MODERADO		L1	1	2	2	1	2	BAJO	13.2.4	Acuerdos de confidencialidad o no revelación.	L1	1	1	1	1	1	MUY BAJO	
5.4.15. [A.19] Divulgación de información	2	4	2	3	MODERADO	No existe planificación de continuidad de seguridad de la información	L1	1	1	3	1	2	BAJO	17.1.1	Planificación de la continuidad de la seguridad de la información.	L3	3	1	1	1	1	MUY BAJO	
5.4.18. [A.24] Denegación de servicio	1	2	2	2	BAJO		L0	0	1	2	2	2	BAJO	18.1.2	Derechos de propiedad intelectual.	L1	1	1	1	1	1	MUY BAJO	

- **SOFTWARE- APLICACIONES INFORMÁTICAS: [SW_APP4]**

Tabla I.13. Matriz de Gestión de Riesgos Actual y Planificado: [SW_APP4]

[SW] SOFTWARE- APLICACIONES INFORMÁTICAS																									
[SW_APP4]	Servidor Digital Ocean																								
AMENAZAS	RIESGO POTENCIAL					CONTROLES/ SALVAGUARDAS EXISTENTES	NIVEL DE MADUREZ - CONTROLES EXISTENTES		RIESGO ACTUAL					CONTROLES/ SALVAGUARDAS SELECCIONADOS			NIVEL DE MADUREZ - CONTROLES ESTABLECIDOS		RIESGO PLANIFICADO						
	RIESGO POTENCIAL POR DIMENSIONES				RIESGO POTENCIAL TOTAL				RIESGO POR DIMENSIONES				RIESGO ACTUAL TOTAL					RIESGO POR DIMENSIONES				RIESGO TOTAL		
	Ri	Rc	Rd	Rt	NIVEL		NIVEL	PUNTOS	Ri	Rc	Rd	Rt	NIVEL				NIVEL	PUNTOS	Ri	Rc	Rd	Rt	NIVEL		
5.2.6. [I.5] Avería de origen físico o lógico	2	3	3	3	MODERADO	Existen controles para la gestión de acceso, donde los usuarios tienen perfiles diferentes según los roles y responsabilidades.	L0	0	2	3	3	2	BAJO	5.1.1	Políticas para la seguridad de la información.		L1	1	1	2	2	2	BAJO		
5.3.2. [E.2] Errores del administrador	3	4	4	4	ALTO		L0	0	3	4	4	3	MODERADO	6.1.4	Contacto con grupos de interés especial.		L2	2	2	2	2	2	BAJO		
5.3.6. [E.8] Difusión de software dañino	2	3	3	3	MODERADO		L0	0	2	3	3	3	MODERADO	9.2.3	Gestión de privilegios de derechos de acceso.		L2	2	3	1	1	2	BAJO		
5.4.3. [A.5] Suplantación de la identidad del usuario	2	2	2	2	BAJO		L0	0	2	2	2	3	MODERADO	13.2.1	Políticas y procedimientos de transferencia de información.		L1	1	4	1	1	2	BAJO		
5.4.4. [A.6] Abuso de privilegios de acceso	3	4	4	4	ALTO	Existe un control que permite el contacto directo con grupos de interés especial en el tema.	L0	0	3	4	4	2	BAJO	16.1.5	Respuesta a incidentes de seguridad de la información.		L2	2	5	2	2	3	MODERADO		
5.4.9. [A.11] Acceso no autorizado	2	3	2	3	MODERADO		L0	0	2	3	2	2	BAJO	17.1.1	Planificación de la continuidad de la seguridad de la información.		L2	2	6	1	0	3	MODERADO		

- **SOFTWARE- APLICACIONES INFORMÁTICAS: [SW_APP2]**

Tabla I.14. Matriz de Gestión de Riesgos Actual y Planificado: [SW_APP2]

[SW] SOFTWARE- APLICACIONES INFORMÁTICAS																									
[SW_APP2]	Servidor FTP																								
AMENAZAS	RIESGO POTENCIAL					CONTROLES/ SALVAGUARDAS EXISTENTES	NIVEL DE MADUREZ - CONTROLES EXISTENTES		RIESGO ACTUAL					CONTROLES/ SALVAGUARDAS SELECCIONADOS		NIVEL DE MADUREZ - CONTROLES ESTABLECIDOS		RIESGO PLANIFICADO					
	RIESGO POTENCIAL DIMENSIONES			RIESGO POTENCIAL TOTAL					RIESGO POR DIMENSIONES			RIESGO ACTUAL TOTAL					RIESGO POR DIMENSIONES			RIESGO TOTAL				
	Ri	Rc	Rd	Rt	NIVEL		NIVEL	PUNTOS	Ri	Rc	Rd	Rt	NIVEL			NIVEL	PUNTOS	Ri	Rc	Rd	Rt	NIVEL		
5.2.6. [I.5] Avería de origen físico o lógico	3	3	3	3	MODERADO	Existen controles para la gestión de acceso, donde los usuarios tienen perfiles diferentes según los roles y responsabilidades. Existen controles referentes a los acuerdos de confidencialidad, para la gestión de información confidencial. Durante la gestión se firman acuerdos de confidencialidad de las partes involucradas. Existe un control que permite el contacto directo con grupos de interés especial en el tema.	L0	0	3	3	3	3	MODERADO	5.1.1	Políticas para la seguridad de la información.	L1	1	2	2	2	2	BAJO
5.3.2. [E.2] Errores del administrador	3	3	1	3	MODERADO		L1	1	2	2	1	2	BAJO	6.1.4	Contacto con grupos de interés especial.	L2	2	1	1	1	1	MUY BAJO	
5.3.6. [E.8] Difusión de software dañino	2	3	3	3	MODERADO		L0	0	2	3	3	3	MODERADO	9.2.3	Gestión de privilegios de derechos de acceso.	L2	2	1	1	1	1	MUY BAJO	
5.3.10. [E.15] Alteración accidental de la información	2	2	1	2	BAJO		L0	0	2	2	1	2	BAJO	12.1.4	Separación de ambientes de desarrollo, pruebas y producción.	L1	1	1	1	1	1	MUY BAJO	
5.3.11. [E.18] Destrucción de información	1	1	1	1	MUY BAJO		L0	0	1	1	1	1	MUY BAJO	12.6.1	Gestión de vulnerabilidades técnicas.	L2	2	1	1	1	1	MUY BAJO	
5.4.3. [A.5] Suplantación de la identidad del usuario	2	2	1	2	BAJO		L0	0	2	2	1	2	BAJO	13.1.2	Seguridad de los servicios de red.	L1	1	1	1	1	1	MUY BAJO	
5.4.4. [A.6] Abuso de privilegios de acceso	4	4	4	4	ALTO		L0	0	4	4	4	3	MODERADO	13.2.1	Políticas y procedimientos de transferencia de información.	L1	1	3	3	3	3	MODERADO	
5.4.9. [A.11] Acceso no autorizado	3	3	2	3	MODERADO		L1	1	2	2	1	2	BAJO	16.1.5	Respuesta a incidentes de seguridad de la información.	L2	2	1	1	1	1	MUY BAJO	
5.4.18. [A.24] Denegación de servicio	1	1	1	1	MUY BAJO		L0	0	1	1	1	1	MUY BAJO	17.1.1	Planificación de la continuidad de la seguridad de la información.	L1	1	1	1	1	1	MUY BAJO	

- **SOFTWARE- APLICACIONES INFORMÁTICAS: [SW_BD2]**

Tabla I.15. Matriz de Gestión de Riesgos Actual y Planificado: [SW_BD2]

[SW] SOFTWARE- APLICACIONES INFORMÁTICAS																										
[SW_BD2]	Servidor de Base de Datos MySQL 8.0																									
AMENAZAS	RIESGO POTENCIAL					CONTROLES/ SALVAGUARDAS EXISTENTES	NIVEL DE MADUREZ - CONTROLES EXISTENTES		RIESGO ACTUAL					CONTROLES/ SALVAGUARDAS SELECCIONADOS			NIVEL DE MADUREZ - CONTROLES ESTABLECIDOS		RIESGO PLANIFICADO						
	RIESGO POTENCIAL DIMENSIONES				RIESGO POTENCIAL TOTAL				RIESGO POR DIMENSIONES				RIESGO ACTUAL TOTAL					RIESGO POR DIMENSIONES				RIESGO TOTAL	
	Ri	Rc	Rd	Rt	NIVEL		NIVEL	PUNTOS	Ri	Rc	Rd	Rt	NIVEL			NIVEL	PUNTOS	Ri	Rc	Rd	Rt	NIVEL	
5.2.6. [I.5] Avería de origen físico o lógico	3	3	3	3	MODERADO	Existen controles para la gestión de acceso, donde los usuarios tienen perfiles diferentes según los roles y responsabilidades. Existen controles referentes a los acuerdos de confidencialidad, para la gestión de información confidencial. Durante la gestión se firman acuerdos de confidencialidad de las partes involucradas. Existe un control que permite la gestión de registros de administración y operación de las bases de datos. No existe planificación de continuidad de seguridad de la información	L0	0	3	3	3	3	MODERADO	5.1.1	Políticas para la seguridad de la información.	L1	1	2	2	2	2	BAJO
5.3.1. [E.1] Errores de los usuarios	4	4	3	4	ALTO		L1	1	3	3	2	3	MODERADO	6.1.1	Roles y responsabilidades de seguridad de la información.	L2	2	1	1	1	1	MUY BAJO
5.3.2. [E.2] Errores del administrador	4	4	4	4	ALTO		L1	1	3	3	3	3	MODERADO	6.1.4	Contacto con grupos de interés especial.	L2	2	1	1	1	1	MUY BAJO
5.3.6. [E.8] Difusión de software dañino	2	3	3	3	MODERADO		L0	0	2	3	3	3	MODERADO	8.2.1	Clasificación de la información.	L1	1	1	2	2	2	BAJO
5.3.10. [E.15] Alteración accidental de la información	2	2	2	2	BAJO		L0	0	2	2	2	2	BAJO	9.1.1	Política de control de accesos.	L2	2	1	1	1	1	MUY BAJO
5.3.11. [E.18] Destrucción de información	1	1	1	1	MUY BAJO		L0	0	1	1	1	1	MUY BAJO	9.4.2	Procedimientos seguros de inicio de sesión.	L2	2	1	1	1	1	MUY BAJO
5.3.12. [E.19] Fugas de información	1	3	2	2	BAJO		L1	1	1	2	1	2	BAJO	12.1.4	Separación de ambientes de desarrollo, pruebas y producción.	L1	1	1	1	1	1	MUY BAJO
5.4.3. [A.5] Suplantación de la identidad del usuario	1	2	2	2	BAJO		L1	1	1	1	1	1	MUY BAJO	12.3.1	Copias de seguridad de la información.	L2	2	1	1	1	1	MUY BAJO
5.4.9. [A.11] Acceso no autorizado	4	4	2	4	ALTO		L1	1	3	3	1	3	MODERADO	12.4.3	Registros de administración y operación.	L1	1	2	2	1	2	BAJO
5.4.13. [A.15] Modificación deliberada de la información	3	3	2	3	MODERADO		L0	0	3	3	2	3	MODERADO	13.2.4	Acuerdos de confidencialidad o no revelación.	L2	2	1	1	1	1	MUY BAJO
5.4.15. [A.19] Divulgación de información	1	4	2	3	MODERADO		L1	1	1	3	1	2	BAJO	17.1.1	Planificación de la continuidad de la seguridad de la información.	L2	2	1	1	1	1	MUY BAJO
5.4.18. [A.24] Denegación de servicio	1	2	2	3	MODERADO		L0	0	1	2	2	2	BAJO	18.1.2	Derechos de propiedad intelectual.	L1	1	1	1	1	1	MUY BAJO

- **SOFTWARE- APLICACIONES INFORMÁTICAS: [SW_APP3]**

Tabla I.16. Matriz de Gestión de Riesgos Actual y Planificado: [SW_APP3]

[SW] SOFTWARE- APLICACIONES INFORMÁTICAS																						
[SW_APP3]	Servidor DNS																					
AMENAZAS	RIESGO POTENCIAL					CONTROLES/ SALVAGUARDAS EXISTENTES	NIVEL DE MADUREZ - CONTROLES EXISTENTES		RIESGO ACTUAL					CONTROLES/ SALVAGUARDAS SELECCIONADOS		NIVEL DE MADUREZ - CONTROLES ESTABLECIDOS		RIESGO PLANIFICADO				
	RIESGO POTENCIAL POR DIMENSIONES			RIESGO POTENCIAL TOTAL					RIESGO POR DIMENSIONES			RIESGO ACTUAL TOTAL						RIESGO POR DIMENSIONES			RIESGO TOTAL	
	Ri	Rc	Rd	Rt	NIVEL		NIVEL	PUNTOS	Ri	Rc	Rd	Rt	NIVEL			NIVEL	PUNTOS	Ri	Rc	Rd	Rt	NIVEL
5.2.6. [I.5] Avería de origen físico o lógico	2	3	3	3	MODERADO	Existen controles para la gestión de acceso, donde los usuarios tienen perfiles diferentes según los roles y responsabilidades. Existe un control que permite el contacto directo con grupos de interés especial en el tema.	L0	0	2	3	3	3	MODERADO	5.1.1	Políticas para la seguridad de la información.	L1	1	1	2	2	2	BAJO
5.3.2. [E.2] Errores del administrador	4	4	4	4	ALTO		L1	1	3	3	3	3	MODERADO	6.1.4	Contacto con grupos de interés especial.	L2	2	1	1	1	1	MUY BAJO
5.3.6. [E.8] Difusión de software dañino	1	3	3	3	MODERADO		L0	0	1	3	3	3	MODERADO	9.2.3	Gestión de privilegios de derechos de acceso.	L2	2	1	1	1	1	MUY BAJO
5.4.3. [A.5] Suplantación de la identidad del usuario	2	2	2	2	BAJO		L0	0	2	2	2	2	BAJO	13.2.1	Políticas y procedimientos de transferencia de información.	L2	2	1	1	1	1	MUY BAJO
5.4.4. [A.6] Abuso de privilegios de acceso	4	4	4	4	ALTO		L1	1	3	3	3	3	MODERADO	16.1.5	Respuesta a incidentes de seguridad de la información.	L2	2	1	1	1	1	MUY BAJO
5.4.9. [A.11] Acceso no autorizado	3	3	2	3	MODERADO		L1	1	2	2	1	2	BAJO	17.1.1	Planificación de la continuidad de la seguridad de la información.	L2	2	1	1	1	1	MUY BAJO
5.4.18. [A.24] Denegación de servicio	1	2	2	2	BAJO		L0	0	1	2	2	2	BAJO			L2	2	1	1	1	1	MUY BAJO

- **SOFTWARE- APLICACIONES INFORMÁTICAS: [SW_BD3]**

Tabla I.17. Matriz de Gestión de Riesgos Actual y Planificado: [SW_BD3] (1/2)

[SW] SOFTWARE- APLICACIONES INFORMÁTICAS																									
[SW_BD3]	Servidor de Base de Datos Postgresql 13																								
AMENAZAS	RIESGO POTENCIAL					CONTROLES/ SALVAGUARDAS EXISTENTES	NIVEL DE MADUREZ - CONTROLES EXISTENTES		RIESGO ACTUAL					CONTROLES/ SALVAGUARDAS SELECCIONADOS		NIVEL DE MADUREZ - CONTROLES ESTABLECIDOS		RIESGO PLANIFICADO				
	RIESGO POTENCIAL POR DIMENSIONES			RIESGO POTENCIAL TOTAL					RIESGO POR DIMENSIONES			RIESGO ACTUAL TOTAL					RIESGO POR DIMENSIONES			RIESGO TOTAL	
	Ri	Rc	Rd	Rt	NIVEL		NIVEL	PUNTOS	Ri	Rc	Rd	Rt	NIVEL			NIVEL	PUNTOS	Ri	Rc	Rd	Rt	NIVEL
5.2.6. [I.5] Avería de origen físico o lógico	1	3	3	3	MODERADO	Existen controles para la gestión de acceso, donde los usuarios tienen perfiles diferentes según los roles y responsabilidades. Existen controles referentes a los acuerdos de confidencialidad, para la gestión de información confidencial. Durante la gestión se firman acuerdos de confidencialidad de las partes involucradas. Existe un control que permite la gestión de registros de administración y operación de las bases de datos.	L0	0	1	3	3	3	MODERADO	5.1.1	Políticas para la seguridad de la información.	L1	1	1	2	2	2	BAJO
5.3.1. [E.1] Errores de los usuarios	4	4	4	4	ALTO		L1	1	3	3	3	3	MODERADO	6.1.1	Roles y responsabilidades de seguridad de la información.	L2	2	1	1	1	1	MUY BAJO
5.3.2. [E.2] Errores del administrador	4	4	4	4	ALTO		L1	1	3	3	3	3	MODERADO	6.1.4	Contacto con grupos de interés especial.	L2	2	1	1	1	1	MUY BAJO
5.3.6. [E.8] Difusión de software dañino	3	2	3	3	MODERADO		L0	0	3	2	3	3	MODERADO	8.2.1	Clasificación de la información.	L2	2	1	1	1	1	MUY BAJO
5.3.10. [E.15] Alteración accidental de la información	4	4	3	4	ALTO		L0	0	4	4	3	4	ALTO	9.1.1	Política de control de accesos.	L2	2	2	2	1	2	BAJO
5.3.11. [E.18] Destrucción de información	1	2	2	2	BAJO		L0	0	1	2	2	2	BAJO	9.4.2	Procedimientos seguros de inicio de sesión.	L1	1	1	1	1	1	MUY BAJO
5.3.12. [E.19] Fugas de información	2	4	3	3	MODERADO		L1	1	1	3	2	2	BAJO	12.1.4	Separación de ambientes de desarrollo, pruebas y producción.	L2	2	1	1	1	1	MUY BAJO
5.4.3. [A.5] Suplantación de la identidad del usuario	1	2	1	2	BAJO		L1	1	1	1	1	1	MUY BAJO	12.3.1	Copias de seguridad de la información.	L2	2	1	1	1	1	MUY BAJO

- **SOFTWARE- APLICACIONES INFORMÁTICAS: [SW_BD3]**

Tabla I.18. Matriz de Gestión de Riesgos Actual y Planificado: [SW_BD3] (2/2)

[SW] SOFTWARE- APLICACIONES INFORMÁTICAS																									
[SW_BD3]	Servidor de Base de Datos Postgresql 13																								
AMENAZAS	RIESGO POTENCIAL					CONTROLES/ SALVAGUARDAS EXISTENTES	NIVEL DE MADUREZ - CONTROLES EXISTENTES		RIESGO ACTUAL					CONTROLES/ SALVAGUARDAS SELECCIONADOS		NIVEL DE MADUREZ - CONTROLES ESTABLECIDOS		RIESGO PLANIFICADO				
	RIESGO POTENCIAL POR DIMENSIONES			RIESGO POTENCIAL TOTAL					RIESGO POR DIMENSIONES			RIESGO ACTUAL TOTAL						RIESGO POR DIMENSIONES				RIESGO TOTAL	
	Ri	Rc	Rd	Rt	NIVEL		NIVEL	PUNTOS	Ri	Rc	Rd	Rt	NIVEL			NIVEL	PUNTOS	Ri	Rc	Rd	Rt	NIVEL	
5.4.9. [A.11] Acceso no autorizado	2	3	2	3	MODERADO		L1	1	1	2	1	2	BAJO	12.4.3	Registros de administración y operación.	L2	2	1	1	1	1	MUY BAJO	
5.4.13. [A.15] Modificación deliberada de la información	3	3	2	3	MODERADO		L0	0	3	3	2	3	MODERADO	13.2.4	Acuerdos de confidencialidad o no revelación.	L1	1	2	2	1	2	BAJO	
5.4.15. [A.19] Divulgación de información	1	4	2	3	MODERADO	No existe planificación de continuidad de seguridad de la información	L1	1	1	3	1	2	BAJO	17.1.1	Planificación de la continuidad de la seguridad de la información.	L2	2	1	1	1	1	MUY BAJO	
5.4.18. [A.24] Denegación de servicio	1	2	2	2	BAJO		L0	0	1	2	2	2	BAJO	18.1.2	Derechos de propiedad intelectual.	L1	1	1	1	1	1	MUY BAJO	

- **SOFTWARE- APLICACIONES INFORMÁTICAS: [SW_AV]**

Tabla I.19. Matriz de Gestión de Riesgos Actual y Planificado: [SW_AV]

[SW] SOFTWARE- APLICACIONES INFORMÁTICAS																								
[SW_AV]	Avast Free Antivirus																							
AMENAZAS	RIESGO POTENCIAL					CONTROLES/ SALVAGUARDAS EXISTENTES	NIVEL DE MADUREZ - CONTROLES EXISTENTES		RIESGO ACTUAL					CONTROLES/ SALVAGUARDAS SELECCIONADOS			NIVEL DE MADUREZ - CONTROLES ESTABLECIDOS		RIESGO PLANIFICADO				
	RIESGO POTENCIAL POR DIMENSIONES			RIESGO POTENCIAL TOTAL					RIESGO POR DIMENSIONES			RIESGO ACTUAL TOTAL							RIESGO POR DIMENSIONES			RIESGO TOTAL	
	Ri	Rc	Rd	Rt	NIVEL		NIVEL	PUNTOS	Ri	Rc	Rd	Rt	NIVEL				NIVEL	PUNTOS	Ri	Rc	Rd	Rt	NIVEL
5.2.6. [I.5] Avería de origen físico o lógico	2	3	3	3	MODERADO	Existen controles para la gestión de acceso, donde los usuarios tienen perfiles diferentes según los roles y responsabilidades.	L0	0	2	3	3	3	MODERADO	5.1.1	Políticas para la seguridad de la información.		L1	1	1	2	2	2	BAJO
5.3.1. [E.1] Errores de los usuarios	3	4	4	4	ALTO		L1	1	2	3	3	3	MODERADO	9.2.3	Gestión de privilegios de derechos de acceso.		L2	2	1	1	1	1	MUY BAJO
5.3.2. [E.2] Errores del administrador	3	4	4	4	ALTO		L1	1	2	3	3	3	MODERADO	9.4.1	Restricción del acceso a la información.		L2	2	1	1	1	1	MUY BAJO
5.3.6. [E.8] Difusión de software dañino	4	4	4	4	ALTO		L1	1	3	3	3	3	MODERADO	12.2.1	Controles contra un malware.		L2	2	1	1	1	1	MUY BAJO
5.3.13. [E.20] Vulnerabilidades de los programas (software)	2	5	5	4	ALTO	Existen políticas de acceso que restringen la instalación de software no autorizado.	L1	1	1	4	4	3	MODERADO	12.4.2	Protección de la información de registro.		L2	2	1	2	2	2	BAJO
5.3.14. [E.21] Errores de mantenimiento / actualización de programas (software)	2	5	5	4	ALTO		L1	1	1	4	4	3	MODERADO	12.6.2	Restricciones en la instalación del software.		L2	2	1	2	2	2	BAJO
5.4.3. [A.5] Suplantación de la identidad del usuario	3	3	3	3	MODERADO		L1	1	2	2	2	2	BAJO	13.2.1	Políticas y procedimientos de transferencia de información.		L2	2	1	1	1	1	MUY BAJO
5.4.4. [A.6] Abuso de privilegios de acceso	4	4	4	4	ALTO		L1	1	3	3	3	3	MODERADO	16.1.2	Informe de los eventos de seguridad de la información.		L2	2	1	1	1	1	MUY BAJO
5.4.9. [A.11] Acceso no autorizado	2	3	2	3	MODERADO		L1	1	1	2	1	2	BAJO	17.1.1	Planificación de la continuidad de la seguridad de la información.		L2	2	1	1	1	1	MUY BAJO

- **SOFTWARE- APLICACIONES INFORMÁTICAS: [SW_APP1]**

Tabla I.20. Matriz de Gestión de Riesgos Actual y Planificado: [SW_APP1] (1/2)

[SW] SOFTWARE- APLICACIONES INFORMÁTICAS																									
[SW_APP1]	Servidor de OwnCloud																								
AMENAZAS	RIESGO POTENCIAL					CONTROLES/ SALVAGUARDAS EXISTENTES	NIVEL DE MADUREZ - CONTROLES EXISTENTES		RIESGO ACTUAL					CONTROLES/ SALVAGUARDAS SELECCIONADOS			NIVEL DE MADUREZ - CONTROLES ESTABLECIDOS		RIESGO PLANIFICADO						
	RIESGO POTENCIAL POR DIMENSIONES				RIESGO POTENCIAL TOTAL				RIESGO POR DIMENSIONES				RIESGO ACTUAL TOTAL						RIESGO POR DIMENSIONES				RIESGO TOTAL	
	Ri	Rc	Rd	Rt	NIVEL		NIVEL	PUNTOS	Ri	Rc	Rd	Rt	NIVEL				NIVEL	PUNTOS	Ri	Rc	Rd	Rt	NIVEL		
5.2.6. [I.5] Avería de origen físico o lógico	3	3	3	3	MODERADO	Existen controles para la gestión de acceso, donde los usuarios tienen perfiles diferentes según los roles y responsabilidades. Existen controles referentes a los acuerdos de confidencialidad, para la gestión de información confidencial. Durante la gestión se firman acuerdos de confidencialidad de las partes involucradas. Existe un control que permite la gestión de registros de administración y operación de las bases de datos.	L0	0	3	3	3	3	MODERADO	5.1.1	Políticas para la seguridad de la información.		L1	1	2	2	2	2	BAJO		
5.3.1. [E.1] Errores de los usuarios	4	4	2	4	ALTO		L1	1	3	3	1	3	MODERADO	6.1.1	Roles y responsabilidades de seguridad de la información.		L2	2	1	1	1	1	MUY BAJO		
5.3.2. [E.2] Errores del administrador	4	4	4	4	ALTO		L1	1	3	3	3	3	MODERADO	6.1.4	Contacto con grupos de interés especial.		L2	2	1	1	1	1	MUY BAJO		
5.3.6. [E.8] Difusión de software dañino	3	3	3	3	MODERADO		L0	0	3	3	3	3	MODERADO	8.2.1	Clasificación de la información.		L2	2	1	1	1	1	MUY BAJO		
5.3.10. [E.15] Alteración accidental de la información	3	3	3	3	MODERADO		L0	0	3	3	3	3	MODERADO	9.1.1	Política de control de accesos.		L2	2	1	1	1	1	MUY BAJO		
5.3.11. [E.18] Destrucción de información	1	1	1	1	MUY BAJO		L0	0	1	1	1	1	MUY BAJO	9.4.2	Procedimientos seguros de inicio de sesión.		L1	1	1	1	1	1	MUY BAJO		
5.3.12. [E.19] Fugas de información	2	4	3	3	MODERADO		L1	1	1	3	2	2	BAJO	12.1.2	Gestión de cambios.		L2	2	1	1	1	1	MUY BAJO		
5.3.14. [E.21] Errores de mantenimiento / actualización de programas (software)	2	4	4	4	ALTO		L1	1	1	3	3	3	MODERADO	12.3.1	Copias de seguridad de la información.		L2	2	1	1	1	1	MUY BAJO		

- **SOFTWARE- APLICACIONES INFORMÁTICAS: [SW_APP1]**

Tabla I.21. Matriz de Gestión de Riesgos Actual y Planificado: [SW_APP1] (2/2)

[SW] SOFTWARE- APLICACIONES INFORMÁTICAS																									
[SW_APP1]	Servidor de OwnCloud																								
AMENAZAS	RIESGO POTENCIAL					CONTROLES/ SALVAGUARDAS EXISTENTES	NIVEL DE MADUREZ - CONTROLES EXISTENTES		RIESGO ACTUAL					CONTROLES/ SALVAGUARDAS SELECCIONADOS		NIVEL DE MADUREZ - CONTROLES ESTABLECIDOS		RIESGO PLANIFICADO					
	RIESGO POTENCIAL POR DIMENSIONES				RIESGO POTENCIAL TOTAL				RIESGO POR DIMENSIONES				RIESGO ACTUAL TOTAL					RIESGO POR DIMENSIONES				RIESGO TOTAL	
	Ri	Rc	Rd	Rt	NIVEL		NIVEL	PUNTOS	Ri	Rc	Rd	Rt	NIVEL			NIVEL	PUNTOS	Ri	Rc	Rd	Rt	NIVEL	
5.4.3. [A.5] Suplantación de la identidad del usuario	3	3	2	3	MODERADO	No existe planificación de continuidad de seguridad de la información No existe un control que brinde respuesta inmediata ante incidentes de seguridad en la nube OwnCloud.	L1	1	2	2	1	2	BAJO	12.4.3	Registros de administración y operación.	L2	2	1	1	1	1	MUY BAJO	
5.4.4. [A.6] Abuso de privilegios de acceso	4	4	4	4	ALTO		L0	0	4	4	4	4	ALTO	13.2.1	Políticas y procedimientos de transferencia de información.	L1	1	3	3	3	3	MODERADO	
5.4.9. [A.11] Acceso no autorizado	3	3	2	3	MODERADO		L1	1	2	2	1	2	BAJO	13.2.4	Acuerdos de confidencialidad o no revelación.	L2	2	1	1	1	1	MUY BAJO	
5.4.13. [A.15] Modificación deliberada de la información	3	3	2	3	MODERADO		L0	0	3	3	2	3	MODERADO	16.1.5	Respuesta a incidentes de seguridad de la información.	L1	1	1	1	1	1	MUY BAJO	
5.4.15. [A.19] Divulgación de información	1	4	1	2	BAJO		L1	1	1	3	1	2	BAJO	17.1.1	Planificación de la continuidad de la seguridad de la información.	L2	2	1	1	1	1	MUY BAJO	
5.4.18. [A.24] Denegación de servicio	1	1	1	1	MUY BAJO		L0	0	1	1	1	2	BAJO	18.1.2	Derechos de propiedad intelectual.	L1	1	1	1	1	1	MUY BAJO	

- **SOFTWARE- APLICACIONES INFORMÁTICAS: [SW_WWW]**

Tabla I.22. Matriz de Gestión de Riesgos Actual y Planificado: [SW_WWW]

[SW] SOFTWARE- APLICACIONES INFORMÁTICAS																									
[SW_WWW]	Servidor Web NGINX																								
AMENAZAS	RIESGO POTENCIAL					CONTROLES/ SALVAGUARDAS EXISTENTES	NIVEL DE MADUREZ - CONTROLES EXISTENTES		RIESGO ACTUAL					CONTROLES/ SALVAGUARDAS SELECCIONADOS		NIVEL DE MADUREZ - CONTROLES ESTABLECIDOS		RIESGO PLANIFICADO					
	RIESGO POTENCIAL POR DIMENSIONES				RIESGO POTENCIAL TOTAL				RIESGO POR DIMENSIONES				RIESGO ACTUAL TOTAL				RIESGO POR DIMENSIONES				RIESGO TOTAL			
	Ri	Rc	Rd	Rt	NIVEL		NIVEL	PUNTOS	Ri	Rc	Rd	Rt	NIVEL			NIVEL	PUNTOS	Ri	Rc	Rd	Rt	NIVEL		
5.2.6. [I.5] Avería de origen físico o lógico	2	2	2	2	BAJO	Existen controles para la gestión de acceso, donde los usuarios tienen perfiles diferentes según los roles y responsabilidades.	L0	0	2	2	2	2	BAJO	5.1.1	Políticas para la seguridad de la información.	L1	1	1	1	1	1	MUY BAJO	
5.3.2. [E.2] Errores del administrador	2	3	3	3	MODERADO		L1	1	1	2	2	2	BAJO	6.1.4	Contacto con grupos de interés especial.	L2	2	1	1	1	1	MUY BAJO	
5.3.6. [E.8] Difusión de software dañino	2	2	2	2	BAJO		L0	0	2	2	2	2	BAJO	9.2.3	Gestión de privilegios de derechos de acceso.	L1	1	1	1	1	1	MUY BAJO	
5.4.3. [A.5] Suplantación de la identidad del usuario	1	1	1	1	MUY BAJO		L0	0	1	1	1	1	MUY BAJO	13.2.1	Políticas y procedimientos de transferencia de información.	L1	1	1	1	1	1	MUY BAJO	
5.4.4. [A.6] Abuso de privilegios de acceso	3	3	3	3	MODERADO	Existe un control que permite el contacto directo con grupos de interés especial en el tema.	L1	1	2	2	2	2	BAJO	16.1.5	Respuesta a incidentes de seguridad de la información.	L2	2	1	1	1	1	MUY BAJO	
5.4.9. [A.11] Acceso no autorizado	2	2	2	2	BAJO		L1	1	1	1	1	1	MUY BAJO	17.1.1	Planificación de la continuidad de la seguridad de la información.	L2	2	1	1	1	1	MUY BAJO	
5.4.18. [A.24] Denegación de servicio	1	1	1	1	MUY BAJO		L0	0	1	1	1	1	MUY BAJO			L1	1	1	1	1	1	MUY BAJO	

- **SOFTWARE- APLICACIONES INFORMÁTICAS: [SW_OS]**

Tabla I.23. Matriz de Gestión de Riesgos Actual y Planificado: [SW_OS] (1/2)

[SW] SOFTWARE- APLICACIONES INFORMÁTICAS																									
[SW_OS]	Windows/Linux																								
AMENAZAS	RIESGO POTENCIAL					CONTROLES/ SALVAGUARDAS EXISTENTES	NIVEL DE MADUREZ - CONTROLES EXISTENTES		RIESGO ACTUAL					CONTROLES/ SALVAGUARDAS SELECCIONADOS		NIVEL DE MADUREZ - CONTROLES ESTABLECIDOS		RIESGO PLANIFICADO					
	RIESGO POTENCIAL POR DIMENSIONES			RIESGO POTENCIAL TOTAL					RIESGO POR DIMENSIONES			RIESGO ACTUAL TOTAL					RIESGO POR DIMENSIONES			RIESGO TOTAL				
	Ri	Rc	Rd	Rt	NIVEL		NIVEL	PUNTOS	Ri	Rc	Rd	Rt	NIVEL			NIVEL	PUNTOS	Ri	Rc	Rd	Rt	NIVEL		
5.2.6. [I.5] Avería de origen físico o lógico	1	3	4	3	MODERADO	Existen controles para la gestión de acceso, donde los usuarios tienen perfiles diferentes según los roles y responsabilidades.	L1	1	1	2	3	2	BAJO	5.1.1	Políticas para la seguridad de la información.	L2	2	1	1	1	1	MUY BAJO	
5.3.1. [E.1] Errores de los usuarios	4	4	4	4	ALTO		L1	1	3	3	3	3	MODERADO	6.1.1	Roles y responsabilidades de seguridad de la información.	L2	2	1	1	1	1	MUY BAJO	
5.3.2. [E.2] Errores del administrador	4	4	4	4	ALTO	Existen controles referentes a los acuerdos de confidencialidad, para la gestión de información confidencial. Durante la gestión se firman acuerdos de confidencialidad de las partes involucradas.	L1	1	3	3	3	3	MODERADO	6.1.4	Contacto con grupos de interés especial.	L2	2	1	1	1	1	MUY BAJO	
5.3.6. [E.8] Difusión de software dañino	2	2	3	3	MODERADO		L0	0	2	2	3	3	MODERADO	9.1.2	Control de acceso a las redes y servicios asociados.	L1	1	1	1	2	2	BAJO	
5.3.10. [E.15] Alteración accidental de la información	1	2	2	2	BAJO		L1	1	1	1	1	1	MUY BAJO	9.1.1	Política de control de accesos.	L2	2	1	1	1	1	MUY BAJO	
5.3.11. [E.18] Destrucción de información	1	1	1	1	MUY BAJO		L0	0	1	1	1	1	MUY BAJO	9.4.2	Procedimientos seguros de inicio de sesión.	L1	1	1	1	1	1	MUY BAJO	
5.3.12. [E.19] Fugas de información	2	4	3	3	MODERADO	Existen controles que permiten la gestión de la seguridad de los servicios de red.	L1	1	1	3	2	2	BAJO	12.2.1	Controles contra un malware.	L2	2	1	1	1	1	MUY BAJO	
5.3.13. [E.20] Vulnerabilidades de los programas (software)	4	4	4	4	ALTO		L0	0	4	4	4	4	ALTO	12.4.1	Registro de eventos.	L1	1	3	3	3	3	MODERADO	

- **SOFTWARE- APLICACIONES INFORMÁTICAS: [SW_OS]**

Tabla I.24. Matriz de Gestión de Riesgos Actual y Planificado: [SW_OS] (2/2)

[SW] SOFTWARE- APLICACIONES INFORMÁTICAS																									
[SW_OS]	Windows/Linux																								
AMENAZAS	RIESGO POTENCIAL					CONTROLES/ SALVAGUARDAS EXISTENTES	NIVEL DE MADUREZ - CONTROLES EXISTENTES		RIESGO ACTUAL					CONTROLES/ SALVAGUARDAS SELECCIONADOS		NIVEL DE MADUREZ - CONTROLES ESTABLECIDOS		RIESGO PLANIFICADO				
	RIESGO POTENCIAL POR DIMENSIONES				RIESGO POTENCIAL TOTAL				RIESGO POR DIMENSIONES				RIESGO ACTUAL TOTAL					RIESGO POR DIMENSIONES				RIESGO TOTAL	
	Ri	Rc	Rd	Rt	NIVEL		NIVEL	PUNTOS	Ri	Rc	Rd	Rt	NIVEL			NIVEL	PUNTOS	Ri	Rc	Rd	Rt	NIVEL	
5.3.14. [E.21] Errores de mantenimiento / actualización de programas (software)	4	4	4	4	ALTO	No existe un control que permite la respuesta ante incidentes de seguridad en caso de fallos del sistema.	L1	1	3	3	3	3	MODERADO	12.5.1	Instalación del software en los sistemas operativos.	L2	2	1	1	1	1	MUY BAJO	
5.4.3. [A.5] Suplantación de la identidad del usuario	1	2	2	2	BAJO		L0	0	1	2	2	2	BAJO	12.6.1	Gestión de vulnerabilidades técnicas.	L1	1	1	1	1	1	MUY BAJO	
5.4.4. [A.6] Abuso de privilegios de acceso	1	4	4	3	MODERADO		L1	1	1	3	3	3	MODERADO	12.6.2	Restricciones en la instalación del software.	L2	2	1	1	1	1	MUY BAJO	
5.4.9. [A.11] Acceso no autorizado	2	3	2	3	MODERADO	No existe planificación de continuidad de seguridad de la información	L0	0	2	3	2	3	MODERADO	12.7.1	Controles de auditoría de los sistemas de información.	L1	1	1	2	1	2	BAJO	
5.4.13. [A.15] Modificación deliberada de la información	3	3	2	3	MODERADO		L0	0	3	3	2	3	MODERADO	16.1.5	Respuesta a incidentes de seguridad de la información.	L2	2	1	1	1	1	MUY BAJO	
5.4.15. [A.19] Divulgación de información	1	4	2	3	MODERADO		L1	1	1	3	1	2	BAJO	17.1.1	Planificación de la continuidad de la seguridad de la información.	L2	2	1	1	1	1	MUY BAJO	
5.4.18. [A.24] Denegación de servicio	1	2	2	2	BAJO		L0	0	1	2	2	2	BAJO	17.1.2	Implementación de la continuidad de seguridad de la información.	L1	1	1	1	1	1	MUY BAJO	

- **SOFTWARE- APLICACIONES INFORMÁTICAS: [SW_ALM]**

Tabla I.25. Matriz de Gestión de Riesgos Actual y Planificado: [SW_ALM]

[SW] SOFTWARE- APLICACIONES INFORMÁTICAS																									
[SW_ALM]	**Google Drive**																								
AMENAZAS	**RIESGO POTENCIAL**					**CONTROLES/ SALVAGUARDAS EXISTENTES**	**NIVEL DE MADUREZ - CONTROLES EXISTENTES**		**RIESGO ACTUAL**					**CONTROLES/ SALVAGUARDAS SELECCIONADOS**		**NIVEL DE MADUREZ - CONTROLES ESTABLECIDOS**		**RIESGO PLANIFICADO**						
	RIESGO POTENCIAL DIMENSIONES			**RIESGO POTENCIAL TOTAL**					**RIESGO POR DIMENSIONES**			**RIESGO ACTUAL TOTAL**							**RIESGO POR DIMENSIONES**			**RIESGO TOTAL**		
	Ri	**Rc**	**Rd**	**Rt**	**NIVEL**		**NIVEL**	**PUNTOS**	**Ri**	**Rc**	**Rd**	**Rt**	**NIVEL**				**NIVEL**	**PUNTOS**	**Ri**	**Rc**	**Rd**	**Rt**	**NIVEL**		
5.3.1. [E.1] Errores de los usuarios	2	3	3	3	MODERADO	Existen controles para la gestión de acceso, donde los usuarios tienen perfiles diferentes según los roles y responsabilidades.	L1	1	1	2	2	2	BAJO	5.1.1	Políticas para la seguridad de la información.		L2	2	1	1	1	1	MUY BAJO		
5.3.2. [E.2] Errores del administrador	3	3	3	3	MODERADO		L1	1	2	2	2	2	BAJO	8.2.1	Clasificación de la información.		L2	2	1	1	1	1	MUY BAJO		
5.3.10. [E.15] Alteración accidental de la información	2	2	2	2	BAJO		L1	1	1	1	1	1	MUY BAJO	8.2.2	Etiquetado de la información.		L2	2	1	1	1	1	MUY BAJO		
5.3.11. [E.18] Destrucción de información	1	1	1	1	MUY BAJO		L0	0	1	1	1	1	MUY BAJO	9.1.1	Política de control de accesos.		L1	1	1	1	1	1	MUY BAJO		
5.3.12. [E.19] Fugas de información	3	3	3	3	MODERADO	Existen controles referentes a los acuerdos de confidencialidad, para la gestión de información confidencial. Durante la gestión se firman acuerdos de confidencialidad de las partes involucradas.	L1	1	2	2	2	2	BAJO	9.2.3	Gestión de privilegios de derechos de acceso.		L2	2	1	1	1	1	MUY BAJO		
5.4.3. [A.5] Suplantación de la identidad del usuario	2	2	2	2	BAJO		L0	0	2	2	2	2	BAJO	12.3.1	Copias de seguridad de la información.		L2	2	1	1	1	1	MUY BAJO		
5.4.4. [A.6] Abuso de privilegios de acceso	3	3	2	3	MODERADO	No existe planificación de continuidad de seguridad de la información	L0	0	3	3	2	3	MODERADO	12.4.2	Protección de la información de registro.		L2	2	1	1	1	1	MUY BAJO		
5.4.9. [A.11] Acceso no autorizado	2	2	2	2	BAJO		L0	0	2	2	2	2	BAJO	13.1.2	Seguridad de los servicios de red.		L1	1	1	1	1	1	MUY BAJO		
5.4.13. [A.15] Modificación deliberada de la información	2	2	2	2	BAJO	No existe un control que brinde respuesta inmediata ante incidentes de seguridad en la nube de Google Drive.	L0	0	2	2	2	2	BAJO	16.1.5	Respuesta a incidentes de seguridad de la información.		L2	2	1	1	1	1	MUY BAJO		
5.4.15. [A.19] Divulgación de información	2	3	2	3	MODERADO		L0	0	2	3	2	3	MODERADO	17.1.1	Planificación de la continuidad de la seguridad de la información.		L2	2	1	1	1	1	MUY BAJO		
5.4.18. [A.24] Denegación de servicio	1	2	2	2	BAJO		L0	0	1	2	2	2	BAJO				L1	1	1	1	1	1	MUY BAJO		

- **SOFTWARE- APLICACIONES INFORMÁTICAS: [SW_OFF]**

Tabla I.26. Matriz de Gestión de Riesgos Actual y Planificado: [SW_OFF]

[SW] SOFTWARE- APLICACIONES INFORMÁTICAS																									
[SW_OFF]	Microsoft Office Professional 2019																								
AMENAZAS	RIESGO POTENCIAL					CONTROLES/ SALVAGUARDAS EXISTENTES	NIVEL DE MADUREZ - CONTROLES EXISTENTES		RIESGO ACTUAL					CONTROLES/ SALVAGUARDAS SELECCIONADOS		NIVEL DE MADUREZ - CONTROLES ESTABLECIDOS		RIESGO PLANIFICADO					
	RIESGO POTENCIAL POR DIMENSIONES			RIESGO POTENCIAL TOTAL					RIESGO POR DIMENSIONES			RIESGO ACTUAL TOTAL					RIESGO POR DIMENSIONES			RIESGO TOTAL	
	Ri	Rc	Rd	Rt	NIVEL		NIVEL	PUNTOS	Ri	Rc	Rd	Rt	NIVEL			NIVEL	PUNTOS	Ri	Rc	Rd	Rt	NIVEL
5.2.6. [I.5] Avería de origen físico o lógico	1	3	3	3	MODERADO	Existen controles para la gestión de acceso, donde los usuarios tienen perfiles diferentes según los roles y responsabilidades.	L1	1	1	2	2	2	BAJO	5.1.1	Políticas para la seguridad de la información.	L2	2	1	1	1	1	MUY BAJO
5.3.1. [E.1] Errores de los usuarios	2	2	2	2	BAJO		L1	1	1	1	1	1	MUY BAJO	9.1.2	Control de acceso a las redes y servicios asociados.	L2	2	1	1	1	1	MUY BAJO
5.3.2. [E.2] Errores del administrador	2	2	2	2	BAJO		L1	1	1	1	1	1	MUY BAJO	9.4.2	Procedimientos seguros de inicio de sesión.	L2	2	1	1	1	1	MUY BAJO
5.3.6. [E.8] Difusión de software dañino	2	2	2	2	BAJO		L0	0	2	2	2	2	BAJO	12.4.1	Registro de eventos.	L1	1	1	1	1	1	MUY BAJO
5.3.14. [E.21] Errores de mantenimiento / actualización de programas (software)	2	2	2	2	BAJO	Existen controles que permiten la gestión de la seguridad de los servicios de red.	L1	1	1	1	1	1	MUY BAJO	12.5.1	Instalación del software en los sistemas operativos.	L2	2	1	1	1	1	MUY BAJO
5.4.3. [A.5] Suplantación de la identidad del usuario	1	2	2	2	BAJO		L0	0	1	2	2	2	BAJO	12.6.1	Gestión de vulnerabilidades técnicas.	L1	1	1	1	1	1	MUY BAJO
5.4.4. [A.6] Abuso de privilegios de acceso	3	3	2	3	MODERADO	Existen controles que permiten la gestión de la seguridad de los servicios de red.	L1	1	2	2	1	2	BAJO	12.6.2	Restricciones en la instalación del software.	L2	2	1	1	1	1	MUY BAJO
5.4.9. [A.11] Acceso no autorizado	2	2	2	2	BAJO		L0	0	2	2	2	2	BAJO	13.1.2	Seguridad de los servicios de red.	L1	1	1	1	1	1	MUY BAJO
5.4.18. [A.24] Denegación de servicio	1	2	2	2	BAJO		L1	1	1	1	1	1	MUY BAJO	16.1.5	Respuesta a incidentes de seguridad de la información.	L2	2	1	1	1	1	MUY BAJO

- **HARDWARE- EQUIPOS INFORMÁTICOS: [HW_HT]**

Tabla I.27. Matriz de Gestión de Riesgos Actual y Planificado: [HW_HT]

[HW] HARDWARE- EQUIPOS INFORMÁTICOS																						
[HW_HT]	Servidor físico HP Proliant DL 360P																					
AMENAZAS	RIESGO POTENCIAL					CONTROLES/ SALVAGUARDAS EXISTENTES	NIVEL DE MADUREZ - CONTROLES EXISTENTES		RIESGO ACTUAL					CONTROLES/ SALVAGUARDAS SELECCIONADOS		NIVEL DE MADUREZ - CONTROLES ESTABLECIDOS		RIESGO PLANIFICADO				
	RIESGO POTENCIAL DIMENSIONES			RIESGO POTENCIAL TOTAL					RIESGO POR DIMENSIONES			RIESGO ACTUAL TOTAL						RIESGO POR DIMENSIONES			RIESGO TOTAL	
	Ri	Rc	Rd	Rt	NIVEL		NIVEL	PUNTOS	Ri	Rc	Rd	Rt	NIVEL			NIVEL	PUNTOS	Ri	Rc	Rd	Rt	NIVEL
5.1.1. [N.1] Fuego	2	3	3	3	MODERADO	Existen controles para la gestión de acceso, donde únicamente el administrador tiene acceso al equipo.	L1	1	1	2	2	2	BAJO	5.1.1	Políticas para la seguridad de la información.	L2	2	1	1	1	1	MUY BAJO
5.1.2. [N.2] Daños por agua	2	3	3	3	MODERADO		L1	1	1	2	2	2	BAJO	5.1.2	Revisión de las políticas para la seguridad de la información.	L2	2	1	1	1	1	MUY BAJO
5.2.3. [I.*] Desastres industriales	2	2	2	2	BAJO		L1	1	1	1	1	1	MUY BAJO	6.1.1	Roles y responsabilidades de seguridad de la información.	L2	2	1	1	1	1	MUY BAJO
5.2.6. [I.5] Avería de origen físico o lógico	2	3	3	3	MODERADO		L0	0	2	3	3	3	MODERADO	8.1.2	Propiedad de los activos.	L1	1	1	2	2	2	BAJO
5.2.7. [I.6] Corte del suministro eléctrico	4	4	5	5	MUY ALTO	Existen controles referentes a las configuraciones de los equipos de red.	L1	1	3	3	4	4	ALTO	8.3.1	Gestión de medios extraíbles.	L2	2	1	1	2	2	BAJO
5.3.2. [E.2] Errores del administrador	4	4	4	4	ALTO		L0	0	4	4	4	4	ALTO	8.3.3	Transferencia de medios físicos.	L1	1	3	3	3	3	MODERADO
5.3.15. [E.23] Errores de mantenimiento / actualización de equipos (hardware)	3	3	3	3	MODERADO		L1	1	2	2	2	2	BAJO	9.1.1	Política de control de accesos.	L2	2	1	1	1	1	MUY BAJO
5.3.17. [E.25] Pérdida de equipos	2	2	2	2	BAJO	Existe un control que permite el contacto directo con grupos de interés especial en el tema.	L0	0	2	2	2	2	BAJO	12.1.3	Gestión de capacidades.	L1	1	1	1	1	1	MUY BAJO
5.4.4. [A.6] Abuso de privilegios de acceso	2	2	2	2	BAJO		L1	1	1	1	1	1	MUY BAJO	12.4.3	Registros de administración y operación.	L2	2	1	1	1	1	MUY BAJO
5.4.9. [A.11] Acceso no autorizado	3	3	2	3	MODERADO		L1	1	2	2	1	2	BAJO	12.6.1	Gestión de vulnerabilidades técnicas.	L2	2	1	1	1	1	MUY BAJO
5.4.17. [A.23] Manipulación de los equipos	2	2	2	2	BAJO	Existe un control que permite la respuesta ante incidentes de seguridad en caso de caída del servicio.	L0	0	2	2	2	2	BAJO	16.1.5	Respuesta a incidentes de seguridad de la información.	L1	1	1	1	1	1	MUY BAJO
5.4.19. [A.25] Robo	2	2	2	2	BAJO		L1	1	1	1	1	1	MUY BAJO	17.1.1	Planificación de la continuidad de la seguridad de la información.	L2	2	1	1	1	1	MUY BAJO

- **HARDWARE - EQUIPOS INFORMÁTICOS: [HW_SW]**

Tabla I.28. Matriz de Gestión de Riesgos Actual y Planificado: [HW_SW]

[HW] HARDWARE- EQUIPOS INFORMÁTICOS																									
[HW_SW]	Switch TP-LINK																								
AMENAZAS	RIESGO POTENCIAL					CONTROLES/ SALVAGUARDAS EXISTENTES	NIVEL DE MADUREZ - CONTROLES EXISTENTES		RIESGO ACTUAL					CONTROLES/ SALVAGUARDAS SELECCIONADOS			NIVEL DE MADUREZ - CONTROLES ESTABLECIDOS		RIESGO PLANIFICADO				
	RIESGO POTENCIAL DIMENSIONES			RIESGO POTENCIAL TOTAL					RIESGO POR DIMENSIONES			RIESGO ACTUAL TOTAL							RIESGO POR DIMENSIONES			RIESGO TOTAL	
	Ri	Rc	Rd	Rt	NIVEL		NIVEL	PUNTOS	Ri	Rc	Rd	Rt	NIVEL				NIVEL	PUNTOS	Ri	Rc	Rd	Rt	NIVEL
5.1.1. [N.1] Fuego	2	3	3	3	MODERADO	Existen controles para la gestión de acceso, donde únicamente el administrador tiene acceso al equipo.	L1	1	1	2	2	2	BAJO	5.1.1	Políticas para la seguridad de la información.		L2	2	1	1	1	1	MUY BAJO
5.1.2. [N.2] Daños por agua	2	2	3	3	MODERADO		L1	1	1	1	2	2	BAJO	5.1.2	Revisión de las políticas para la seguridad de la información.		L2	2	1	1	1	1	MUY BAJO
5.2.3. [I.*] Desastres industriales	2	2	2	2	BAJO		L1	1	1	1	1	1	MUY BAJO	6.1.1	Roles y responsabilidades de seguridad de la información.		L2	2	1	1	1	1	MUY BAJO
5.2.6. [I.5] Avería de origen físico o lógico	3	2	3	3	MODERADO		L0	0	3	2	3	3	MODERADO	8.1.3	Uso aceptable de los activos.		L1	1	2	1	2	2	BAJO
5.2.7. [I.6] Corte del suministro eléctrico	4	5	5	5	MUY ALTO	Existen controles referentes a las configuraciones de los equipos de red.	L1	1	3	4	4	4	ALTO	8.3.1	Gestión de medios extraíbles.		L2	2	1	2	2	2	BAJO
5.3.2. [E.2] Errores del administrador	3	4	4	4	ALTO		L0	0	3	4	4	4	ALTO	8.3.3	Transferencia de medios físicos.		L1	1	2	3	3	3	MODERADO
5.3.15. [E.23] Errores de mantenimiento / actualización de equipos (hardware)	2	3	3	3	MODERADO		L1	1	1	2	2	2	BAJO	9.1.1	Política de control de accesos.		L2	2	1	1	1	1	MUY BAJO
5.3.17. [E.25] Pérdida de equipos	2	2	2	2	BAJO	Existe un control que permite la respuesta ante incidentes de seguridad en caso de caída del servicio.	L0	0	2	2	2	2	BAJO	9.4.2	Procedimientos seguros de inicio de sesión.		L1	1	1	1	1	1	MUY BAJO
5.4.4. [A.6] Abuso de privilegios de acceso	2	2	2	2	BAJO		L1	1	1	1	1	1	MUY BAJO	12.4.3	Registros de administración y operación.		L2	2	1	1	1	1	MUY BAJO
5.4.9. [A.11] Acceso no autorizado	3	3	2	3	MODERADO		L1	1	2	2	1	2	BAJO	12.6.1	Gestión de vulnerabilidades técnicas.		L2	2	1	1	1	1	MUY BAJO
5.4.17. [A.23] Manipulación de los equipos	2	2	1	2	BAJO	No existe planificación de continuidad de seguridad de la información	L0	0	2	2	1	2	BAJO	16.1.5	Respuesta a incidentes de seguridad de la información.		L1	1	1	1	1	1	MUY BAJO
5.4.19. [A.25] Robo	2	2	2	2	BAJO		L1	1	1	1	1	1	MUY BAJO	17.1.1	Planificación de la continuidad de la seguridad de la información.		L2	2	1	1	1	1	MUY BAJO

- **HARDWARE - EQUIPOS INFORMÁTICOS: [HW_MV2]**

Tabla I.29. Matriz de Gestión de Riesgos Actual y Planificado: [HW_MV2] (1/2)

[HW] HARDWARE- EQUIPOS INFORMÁTICOS																							
[HW_MV2]	Teléfonos móviles																						
AMENAZAS	RIESGO POTENCIAL					CONTROLES/ SALVAGUARDAS EXISTENTES	NIVEL DE MADUREZ - CONTROLES EXISTENTES		RIESGO ACTUAL					CONTROLES/ SALVAGUARDAS SELECCIONADOS		NIVEL DE MADUREZ - CONTROLES ESTABLECIDOS		RIESGO PLANIFICADO					
	RIESGO POTENCIAL POR DIMENSIONES			RIESGO POTENCIAL TOTAL					RIESGO POR DIMENSIONES			RIESGO ACTUAL TOTAL						RIESGO POR DIMENSIONES			RIESGO TOTAL	
	Ri	Rc	Rd	Rt	NIVEL		NIVEL	PUNTOS	Ri	Rc	Rd	Rt	NIVEL			NIVEL	PUNTOS	Ri	Rc	Rd	Rt	NIVEL
5.1.1. [N.1] Fuego	2	3	3	3	MODERADO	Existen controles para la gestión de acceso, donde los usuarios tienen perfiles diferentes según los roles y responsabilidades. Existen controles referentes a los acuerdos de confidencialidad, para la gestión de información confidencial. Durante la gestión se firman acuerdos de confidencialidad de las partes involucradas. No existen controles que gestiones la devolución de los teléfonos móviles.	L1	1	1	2	2	2	BAJO	5.1.1	Políticas para la seguridad de la información.	L2	2	1	1	1	1	MUY BAJO
5.1.2. [N.2] Daños por agua	2	3	3	3	MODERADO		L0	0	2	3	3	3	MODERADO	6.1.1	Roles y responsabilidades de seguridad de la información.	L2	2	1	1	1	1	MUY BAJO
5.2.3. [I.*] Desastres industriales	2	2	2	2	BAJO		L1	1	1	1	1	1	MUY BAJO	6.2.1	Política de dispositivo móvil.	L2	2	1	1	1	1	MUY BAJO
5.2.6. [I.5] Avería de origen físico o lógico	2	3	3	3	MODERADO		L0	0	2	3	3	3	MODERADO	8.1.4	Devolución de activos.	L1	1	1	2	2	2	BAJO
5.2.7. [I.6] Corte del suministro eléctrico	2	3	4	3	MODERADO		L1	1	1	2	3	2	BAJO	8.3.1	Gestión de medios extraíbles.	L2	2	1	1	1	1	MUY BAJO
5.3.1. [E.1] Errores de los usuarios	3	4	5	4	ALTO		L0	0	3	4	5	4	ALTO	8.3.3	Transferencia de medios físicos.	L1	1	2	3	4	3	MODERADO
5.3.2. [E.2] Errores del administrador	3	4	5	4	ALTO		L1	1	2	3	4	3	MODERADO	9.1.1	Política de control de accesos.	L2	2	1	1	2	2	BAJO
5.3.12. [E.19] Fugas de información	5	5	5	5	MUY ALTO		L0	0	5	5	5	5	MUY ALTO	9.4.2	Procedimientos seguros de inicio de sesión.	L1	1	4	4	4	4	ALTO

- **HARDWARE - EQUIPOS INFORMÁTICOS: [HW_MV2]**

Tabla I.30. Matriz de Gestión de Riesgos Actual y Planificado: [HW_MV2] (2/2)

[HW] HARDWARE- EQUIPOS INFORMÁTICOS																							
[HW_MV2]	Teléfonos móviles																						
AMENAZAS	RIESGO POTENCIAL					CONTROLES/ SALVAGUARDAS EXISTENTES	NIVEL DE MADUREZ - CONTROLES EXISTENTES		RIESGO ACTUAL					CONTROLES/ SALVAGUARDAS SELECCIONADOS		NIVEL DE MADUREZ - CONTROLES ESTABLECIDOS		RIESGO PLANIFICADO				
	RIESGO POTENCIAL POR DIMENSIONES			RIESGO POTENCIAL TOTAL					RIESGO POR DIMENSIONES			RIESGO ACTUAL TOTAL					RIESGO POR DIMENSIONES			RIESGO TOTAL	
	Ri	Rc	Rd	Rt	NIVEL		NIVEL	PUNTOS	Ri	Rc	Rd	Rt	NIVEL			NIVEL	PUNTOS	Ri	Rc	Rd	Rt	NIVEL
5.3.15. [E.23] Errores de mantenimiento / actualización de equipos (hardware)	4	4	4	4	ALTO	No existen políticas que restrinja la transferencia de información confidencial.	L1	1	3	3	3	3	MODERADO	12.2.1	Controles contra un malware.	L2	2	1	1	1	1	MUY BAJO
5.3.17. [E.25] Pérdida de equipos	2	4	4	4	ALTO		L0	0	2	4	4	4	ALTO	12.3.1	Copias de seguridad de la información.	L1	1	1	3	3	3	MODERADO
5.4.3. [A.5] Suplantación de la identidad del usuario	2	3	3	3	MODERADO	No existen controles que eviten un ataque de denegación de servicio.	L1	1	1	2	2	2	BAJO	12.6.1	Gestión de vulnerabilidades técnicas.	L2	2	1	1	1	1	MUY BAJO
5.4.4. [A.6] Abuso de privilegios de acceso	2	3	3	3	MODERADO		L0	0	2	3	3	3	MODERADO	13.2.1	Políticas y procedimientos de transferencia de información.	L1	1	1	2	2	2	BAJO
5.4.9. [A.11] Acceso no autorizado	2	3	2	3	MODERADO	Existe un control que especifica la sanción en el caso de pérdida de los equipos.	L1	1	1	2	1	2	BAJO	13.2.3	Mensajería electrónica.	L2	2	1	1	1	1	MUY BAJO
5.4.17. [A.23] Manipulación de los equipos	3	4	4	4	ALTO		L0	0	3	4	4	4	ALTO	13.2.4	Acuerdos de confidencialidad o no revelación.	L1	1	2	3	3	3	MODERADO
5.4.19. [A.25] Robo	4	4	4	4	ALTO	No existe planificación de continuidad de seguridad de la información	L1	1	3	3	3	3	MODERADO	16.1.5	Respuesta a incidentes de seguridad de la información.	L2	2	1	1	1	1	MUY BAJO

- **HARDWARE- EQUIPOS INFORMÁTICOS: [HW_PC]**

Tabla I.31. Matriz de Gestión de Riesgos Actual y Planificado: [HW_PC]

[HW] HARDWARE- EQUIPOS INFORMÁTICOS																									
[HW_PC]	Computadoras de escritorio																								
AMENAZAS	RIESGO POTENCIAL					CONTROLES/ SALVAGUARDAS EXISTENTES	NIVEL DE MADUREZ - CONTROLES EXISTENTES		RIESGO ACTUAL					CONTROLES/ SALVAGUARDAS SELECCIONADOS			NIVEL DE MADUREZ - CONTROLES ESTABLECIDOS		RIESGO PLANIFICADO						
	RIESGO POTENCIAL DIMENSIONES			RIESGO POTENCIAL TOTAL					RIESGO POR DIMENSIONES			RIESGO ACTUAL TOTAL							RIESGO POR DIMENSIONES				RIESGO TOTAL	
	Ri	Rc	Rd	Rt	NIVEL		NIVEL	PUNTOS	Ri	Rc	Rd	Rt	NIVEL				NIVEL	PUNTOS	Ri	Rc	Rd	Rt	NIVEL		
5.1.1. [N.1] Fuego	1	2	3	2	BAJO	Existen controles para la gestión de acceso, donde los usuarios tienen perfiles diferentes según los roles y responsabilidades.	L1	1	1	1	2	2	BAJO	5.1.1	Políticas para la seguridad de la información.		L2	2	1	1	1	1	MUY BAJO		
5.1.2. [N.2] Daños por agua	2	2	3	3	MODERADO		L1	1	1	1	2	2	BAJO	6.1.1	Roles y responsabilidades de seguridad de la información.		L2	2	1	1	1	1	MUY BAJO		
5.2.3. [I.*] Desastres industriales	1	1	2	2	BAJO		L1	1	1	1	1	1	MUY BAJO	8.1.3	Uso aceptable de los activos.		L2	2	1	1	1	1	MUY BAJO		
5.2.6. [I.5] Avería de origen físico o lógico	2	2	3	3	MODERADO	Existen controles referentes a las configuraciones de los equipos de red.	L0	0	2	2	3	3	MODERADO	8.3.1	Gestión de medios extraíbles.		L1	1	1	1	2	2	BAJO		
5.2.7. [I.6] Corte del suministro eléctrico	3	4	4	4	ALTO		L1	1	2	3	3	3	MODERADO	8.3.3	Transferencia de medios físicos.		L2	2	1	1	1	1	MUY BAJO		
5.3.1. [E.1] Errores de los usuarios	4	4	4	4	ALTO		L0	0	4	4	4	4	ALTO	9.1.1	Política de control de accesos.		L1	1	3	3	3	3	MODERADO		
5.3.2. [E.2] Errores del administrador	4	4	4	4	ALTO	No existen políticas que restrinja la transferencia de información confidencial.	L1	1	3	3	3	3	MODERADO	9.1.2	Control de acceso a las redes y servicios asociados.		L2	2	1	1	1	1	MUY BAJO		
5.3.15. [E.23] Errores de mantenimiento / actualización de equipos (hardware)	3	4	4	4	ALTO		L0	0	3	4	4	4	ALTO	9.4.2	Procedimientos seguros de inicio de sesión.		L1	1	2	3	3	3	MODERADO		
5.3.17. [E.25] Pérdida de equipos	4	4	4	4	ALTO	No existen controles que eviten el abuso de privilegios.	L1	1	3	3	3	3	MODERADO	12.2.1	Controles contra un malware.		L2	2	1	1	1	1	MUY BAJO		
5.4.3. [A.5] Suplantación de la identidad del usuario	3	3	3	3	MODERADO		L1	1	2	2	2	2	BAJO	12.3.1	Copias de seguridad de la información.		L2	2	1	1	1	1	MUY BAJO		
5.4.4. [A.6] Abuso de privilegios de acceso	2	3	2	3	MODERADO	No existe un control que gestione los errores de mantenimiento y actualización de equipos.	L1	1	1	2	1	2	BAJO	12.6.1	Gestión de vulnerabilidades técnicas.		L1	1	1	1	1	1	MUY BAJO		
5.4.9. [A.11] Acceso no autorizado	3	3	2	3	MODERADO		L1	1	2	2	1	2	BAJO	13.2.1	Políticas y procedimientos de transferencia de información.		L2	2	1	1	1	1	MUY BAJO		
5.4.17. [A.23] Manipulación de los equipos	4	4	3	4	ALTO	No existe planificación de continuidad de seguridad de la información	L1	1	3	3	2	3	MODERADO	13.2.4	Acuerdos de confidencialidad o no revelación.		L1	1	2	2	1	2	BAJO		
5.4.19. [A.25] Robo	1	1	2	2	BAJO		L1	1	1	1	1	1	MUY BAJO	16.1.5	Respuesta a incidentes de seguridad.		L2	2	1	1	1	1	MUY BAJO		

- **HARDWARE- EQUIPOS INFORMÁTICOS: [HW_MV1]**

Tabla I.32. Matriz de Gestión de Riesgos Actual y Planificado: [HW_MV1] (1/2)

[HW] HARDWARE- EQUIPOS INFORMÁTICOS																							
[HW_MV1]	Computadoras Portátiles																						
AMENAZAS	RIESGO POTENCIAL					CONTROLES/ SALVAGUARDAS EXISTENTES	NIVEL DE MADUREZ - CONTROLES EXISTENTES		RIESGO ACTUAL					CONTROLES/ SALVAGUARDAS SELECCIONADOS		NIVEL DE MADUREZ - CONTROLES ESTABLECIDOS		RIESGO PLANIFICADO				
	RIESGO POTENCIAL DIMENSIONES			RIESGO POTENCIAL TOTAL					RIESGO POR DIMENSIONES			RIESGO ACTUAL TOTAL						RIESGO POR DIMENSIONES			RIESGO TOTAL	
	Ri	Rc	Rd	Rt	NIVEL		NIVEL	PUNTOS	Ri	Rc	Rd	Rt	NIVEL			NIVEL	PUNTOS	Ri	Rc	Rd	Rt	NIVEL
5.1.1. [N.1] Fuego	2	2	3	3	MODERADO	Existen controles para la gestión de acceso, donde los usuarios tienen perfiles diferentes según los roles y responsabilidades.	L1	1	1	1	2	2	BAJO	5.1.1	Políticas para la seguridad de la información.	L2	2	1	1	1	1	MUY BAJO
5.1.2. [N.2] Daños por agua	2	2	3	3	MODERADO		L1	1	1	1	2	2	BAJO	6.1.1	Roles y responsabilidades de seguridad de la información.	L2	2	1	1	1	1	MUY BAJO
5.2.3. [I.*] Desastres industriales	1	1	2	2	BAJO		L1	1	1	1	1	1	MUY BAJO	6.2.1	Política de dispositivo móvil.	L2	2	1	1	1	1	MUY BAJO
5.2.6. [I.5] Avería de origen físico o lógico	2	3	3	3	MODERADO		L0	0	2	3	3	3	MODERADO	8.1.3	Uso aceptable de los activos.	L1	1	1	2	2	2	BAJO
5.2.7. [I.6] Corte del suministro eléctrico	4	4	4	4	ALTO	Existen controles referentes a las configuraciones de los equipos de red.	L1	1	3	3	3	3	MODERADO	8.3.1	Gestión de medios extraíbles.	L2	2	1	1	1	1	MUY BAJO
5.3.1. [E.1] Errores de los usuarios	4	4	2	4	ALTO		L0	0	4	4	2	4	ALTO	8.3.3	Transferencia de medios físicos.	L1	1	3	3	1	3	MODERADO
5.3.2. [E.2] Errores del administrador	4	4	3	4	ALTO	No existen controles que gestionen la devolución de computadoras portátiles.	L1	1	3	3	2	3	MODERADO	9.1.1	Política de control de accesos.	L2	2	1	1	1	1	MUY BAJO

- **HARDWARE- EQUIPOS INFORMÁTICOS: [HW_MV1]**

Tabla I.33. Matriz de Gestión de Riesgos Actual y Planificado: [HW_MV1] (2/2)

[HW] HARDWARE- EQUIPOS INFORMÁTICOS																						
[HW_MV1]	Computadoras Portátiles																					
AMENAZAS	RIESGO POTENCIAL					CONTROLES/ SALVAGUARDAS EXISTENTES	NIVEL DE MADUREZ - CONTROLES EXISTENTES		RIESGO ACTUAL					CONTROLES/ SALVAGUARDAS SELECCIONADOS		NIVEL DE MADUREZ - CONTROLES ESTABLECIDOS		RIESGO PLANIFICADO				
	RIESGO POTENCIAL DIMENSIONES			RIESGO POTENCIAL TOTAL					RIESGO POR DIMENSIONES			RIESGO ACTUAL TOTAL						RIESGO POR DIMENSIONES			RIESGO TOTAL	
	Ri	Rc	Rd	Rt	NIVEL		NIVEL	PUNTOS	Ri	Rc	Rd	Rt	NIVEL			NIVEL	PUNTOS	Ri	Rc	Rd	Rt	NIVEL
5.3.15. [E.23] Errores de mantenimiento / actualización de equipos (hardware)	4	4	4	4	ALTO	No existen políticas que restrinja la transferencia de información confidencial.	L0	0	4	4	4	4	ALTO	9.4.2	Procedimientos seguros de inicio de sesión.	L1	1	3	3	3	3	MODERADO
5.3.17. [E.25] Pérdida de equipos	2	4	4	4	ALTO		L1	1	1	3	3	3	MODERADO	12.2.1	Controles contra un malware.	L2	2	1	1	1	1	MUY BAJO
5.4.3. [A.5] Suplantación de identidad.	3	3	3	3	MODERADO		L1	1	2	2	2	2	BAJO	12.3.1	Copias de seguridad de la información.	L2	2	1	1	1	1	MUY BAJO
5.4.4. [A.6] Abuso de privilegios de acceso	3	3	2	3	MODERADO	No existen controles que eviten un ataque de denegación de servicio.	L0	0	3	3	2	3	MODERADO	12.6.1	Gestión de vulnerabilidades técnicas.	L1	1	2	2	1	2	BAJO
5.4.9. [A.11] Acceso no autorizado	2	3	2	3	MODERADO	Existe un control que especifica la sanción en el caso de pérdida de los equipos.	L1	1	1	2	1	2	BAJO	13.2.1	Políticas y procedimientos de transferencia de información.	L2	2	1	1	1	1	MUY BAJO
5.4.17. [A.23] Manipulación de los equipos	4	4	3	4	ALTO		L0	0	4	4	3	4	ALTO	13.2.4	Acuerdos de confidencialidad o no revelación.	L1	1	3	3	2	2	BAJO
5.4.19. [A.25] Robo	4	4	4	4	ALTO	No existe planificación de continuidad de seguridad de la información	L0	0	4	4	4	4	ALTO	16.1.5	Respuesta a incidentes de seguridad.	L2	2	2	2	2	2	BAJO

- **HARDWARE- EQUIPOS INFORMÁTICOS: [HW_WAP]**

Tabla I.34. Matriz de Gestión de Riesgos Actual y Planificado: [HW_WAP]

[HW] HARDWARE- EQUIPOS INFORMÁTICOS																							
[HW_WAP]	Punto de Acceso																						
AMENAZAS	RIESGO POTENCIAL					CONTROLES/ SALVAGUARDAS EXISTENTES	NIVEL DE MADUREZ - CONTROLES EXISTENTES		RIESGO ACTUAL					CONTROLES/ SALVAGUARDAS SELECCIONADOS			NIVEL DE MADUREZ - CONTROLES ESTABLECIDOS		RIESGO PLANIFICADO				
	RIESGO POTENCIAL POR DIMENSIONES			RIESGO POTENCIAL TOTAL					RIESGO POR DIMENSIONES			RIESGO ACTUAL TOTAL							RIESGO POR DIMENSIONES			RIESGO TOTAL	
	Ri	Rc	Rd	Rt	NIVEL		NIVEL	PUNTOS	Ri	Rc	Rd	Rt	NIVEL				NIVEL	PUNTOS	Ri	Rc	Rd	Rt	NIVEL
5.1.1. [N.1] Fuego	2	2	2	2	BAJO		L1	1	1	1	1	2	BAJO	5.1.1	Políticas para la seguridad de la información.		L2	2	1	1	1	1	MUY BAJO
5.1.2. [N.2] Daños por agua	3	3	4	4	ALTO	Existen controles para la gestión de acceso, donde únicamente el administrador tiene acceso al equipo.	L1	1	2	2	3	3	MODERADO	6.1.1	Roles y responsabilidades de seguridad de la información.		L2	2	1	1	1	1	MUY BAJO
5.2.3. [I.*] Desastres industriales	2	2	2	2	BAJO		L1	1	1	1	1	1	MUY BAJO	8.1.3	Uso aceptable de los activos.		L2	2	1	1	1	1	MUY BAJO
5.2.6. [I.5] Avería de origen físico o lógico	2	3	3	3	MODERADO		L0	0	2	3	3	3	MODERADO	9.1.1	Política de control de accesos.		L1	1	1	2	2	2	BAJO
5.2.7. [I.6] Corte del suministro eléctrico	4	4	4	4	ALTO	Existe un procedimiento de control de acceso a la red, mediante el uso de contraseñas.	L0	0	4	4	4	4	ALTO	9.1.2	Control de acceso a las redes y servicios asociados.		L2	2	2	2	2	2	BAJO
5.4.4. [A.6] Abuso de privilegios de acceso	2	3	2	3	MODERADO		L0	0	2	3	2	3	MODERADO	12.4.1	Registro de eventos.		L1	1	1	2	1	2	BAJO
5.4.9. [A.11] Acceso no autorizado	3	3	2	3	MODERADO	No existe una política que indique el uso aceptable de un activo.	L1	1	2	2	1	2	BAJO	13.1.1	Controles de red.		L2	2	1	1	1	1	MUY BAJO
5.4.17. [A.23] Manipulación de los equipos	3	3	2	3	MODERADO		L0	0	3	3	2	3	MODERADO	16.1.5	Respuesta a incidentes de seguridad de la información.		L1	1	2	2	1	2	BAJO
5.4.19. [A.25] Robo	2	2	2	2	BAJO	No existe planificación de continuidad de seguridad de la información	L0	0	2	2	2	2	BAJO	17.1.1	Planificación de la continuidad de la seguridad de la información.		L2	2	1	1	1	1	MUY BAJO

- **HARDWARE- EQUIPOS INFORMÁTICOS: [HW_PT]**

Tabla I.35. Matriz de Gestión de Riesgos Actual y Planificado: [HW_PT]

[HW] HARDWARE- EQUIPOS INFORMÁTICOS																						
[HW_PT]	Impresoras																					
AMENAZAS	RIESGO POTENCIAL					CONTROLES/ SALVAGUARDAS EXISTENTES	NIVEL DE MADUREZ - CONTROLES EXISTENTES		RIESGO ACTUAL					CONTROLES/ SALVAGUARDAS SELECCIONADOS		NIVEL DE MADUREZ - CONTROLES ESTABLECIDOS		RIESGO PLANIFICADO				
	RIESGO POTENCIAL POR DIMENSIONES			RIESGO POTENCIAL TOTAL					RIESGO POR DIMENSIONES			RIESGO ACTUAL TOTAL					RIESGO POR DIMENSIONES			RIESGO TOTAL	
	Ri	Rc	Rd	Rt	NIVEL		NIVEL	PUNTOS	Ri	Rc	Rd	Rt	NIVEL			NIVEL	PUNTOS	Ri	Rc	Rd	Rt	NIVEL
5.1.1. [N.1] Fuego	1	1	1	1	MUY BAJO	Existe un control que permite la gestión de acceso a este dispositivo.	L1	1	1	1	1	1	MUY BAJO	5.1.1	Políticas para la seguridad de la información.	L2	2	1	1	1	1	MUY BAJO
5.1.2. [N.2] Daños por agua	1	1	2	2	BAJO		L0	0	1	1	2	2	BAJO	8.1.3	Uso aceptable de los activos.	L1	1	1	1	1	1	MUY BAJO
5.2.3. [I.*] Desastres industriales	1	1	1	1	MUY BAJO		L1	1	1	1	1	1	MUY BAJO	8.3.1	Gestión de medios extraíbles.	L2	2	1	1	1	1	MUY BAJO
5.2.6. [I.5] Avería de origen físico o lógico	1	2	2	2	BAJO		L0	0	1	2	2	2	BAJO	8.3.3	Transferencia de medios físicos.	L1	1	1	1	1	1	MUY BAJO
5.2.7. [I.6] Corte del suministro eléctrico	2	2	2	2	BAJO	No existe una política que indique el uso aceptable de un activo.	L1	1	1	1	1	1	MUY BAJO	12.4.1	Registro de eventos.	L2	2	1	1	1	1	MUY BAJO
5.4.4. [A.6] Abuso de privilegios de acceso	1	2	2	2	BAJO		L0	0	1	2	2	2	BAJO	12.6.1	Gestión de vulnerabilidades técnicas.	L1	1	1	1	1	1	MUY BAJO
5.4.9. [A.11] Acceso no autorizado	2	2	2	2	BAJO		L1	1	1	1	1	1	MUY BAJO	13.1.1	Controles de red.	L2	2	1	1	1	1	MUY BAJO
5.4.17. [A.23] Manipulación de los equipos	2	2	2	2	BAJO	Existen controles referentes a las configuraciones de los equipos de red.	L0	0	2	2	2	2	BAJO	13.1.2	Seguridad de los servicios de red.	L1	1	1	1	1	1	MUY BAJO
5.4.19. [A.25] Robo	1	1	1	1	MUY BAJO		L0	0	1	1	1	1	MUY BAJO	16.1.5	Respuesta a incidentes de seguridad de la información.	L2	2	1	1	1	1	MUY BAJO

- **REDES DE COMUNICACIONES: [COM_INT]**

Tabla I.36. Matriz de Gestión de Riesgos Actual y Planificado: [COM_INT]

[COM] REDES DE COMUNICACIONES																									
[COM_INT]	Internet Fibra Óptica																								
AMENAZAS	RIESGO POTENCIAL					CONTROLES/ SALVAGUARDAS EXISTENTES	NIVEL DE MADUREZ - CONTROLES EXISTENTES		RIESGO ACTUAL					CONTROLES/ SALVAGUARDAS SELECCIONADOS			NIVEL DE MADUREZ - CONTROLES ESTABLECIDOS		RIESGO PLANIFICADO						
	RIESGO POTENCIAL DIMENSIONES			RIESGO POTENCIAL TOTAL					RIESGO POR DIMENSIONES			RIESGO ACTUAL TOTAL							RIESGO POR DIMENSIONES				RIESGO TOTAL	
	Ri	Rc	Rd	Rt	NIVEL		NIVEL	PUNTOS	Ri	Rc	Rd	Rt	NIVEL				NIVEL	PUNTOS	Ri	Rc	Rd	Rt	NIVEL	
5.2.9. [I.8] Fallo de servicios de comunicaciones	2	4	5	4	ALTO	Existe un control que permite el contacto directo con grupos de interés especial en el tema.	L1	1	1	3	4	3	MODERADO	5.1.1	Políticas para la seguridad de la información.		L2	2	1	1	1	1	MUY BAJO	
5.3.2. [E.2] Errores del administrador	3	4	4	4	ALTO		L1	1	2	3	3	3	MODERADO	6.1.1	Roles y responsabilidades de seguridad de la información.		L2	2	1	1	1	1	MUY BAJO	
5.3.11. [E.18] Destrucción de información	1	2	2	2	BAJO		L1	1	1	1	1	1	MUY BAJO	8.1.3	Uso aceptable de los activos.		L2	2	1	1	1	1	MUY BAJO	
5.3.12. [E.19] Fugas de información	1	2	2	2	BAJO		L0	0	1	2	2	2	BAJO	9.1.1	Política de control de accesos.		L1	1	1	1	1	1	MUY BAJO	
5.4.3. [A.5] Suplantación de la identidad del usuario	2	3	2	3	MODERADO	No existe un backup de este servicio.	L1	1	1	2	1	2	BAJO	9.1.2	Control de acceso a las redes y servicios asociados.		L2	2	1	1	1	1	MUY BAJO	
5.4.4. [A.6] Abuso de privilegios de acceso	2	3	3	3	MODERADO		L0	0	2	3	3	3	MODERADO	12.4.1	Registro de eventos.		L1	1	1	2	2	2	BAJO	
5.4.9. [A.11] Acceso no autorizado	2	4	4	4	ALTO		L1	1	1	3	3	3	MODERADO	13.1.1	Controles de red.		L2	2	1	1	1	1	MUY BAJO	
5.4.10. [A.12] Análisis de tráfico	4	4	3	4	ALTO	Existe un procedimiento a seguir en el caso de fallos del servicio.	L0	0	4	4	3	4	ALTO	16.1.5	Respuesta a incidentes de seguridad de la información.		L1	1	3	3	2	3	MODERADO	
5.4.13. [A.15] Modificación deliberada de la información	2	2	2	2	BAJO		L1	1	1	1	1	1	MUY BAJO	17.1.1	Planificación de la continuidad de la seguridad de la información.		L2	2	1	1	1	1	MUY BAJO	
5.4.15. [A.19] Divulgación de información	1	2	2	2	BAJO	No existe planificación de continuidad de seguridad de la información	L0	0	1	2	2	2	BAJO				L1	1	1	1	1	1	MUY BAJO	
5.4.18. [A.24] Denegación de servicio	2	3	3	3	MODERADO		L0	0	2	3	3	3	MODERADO				L2	2	1	1	1	1	MUY BAJO	

- **REDES DE COMUNICACIONES: [COM_LAN]**

Tabla I.37. Matriz de Gestión de Riesgos Actual y Planificado: [COM_LAN]

[COM] REDES DE COMUNICACIONES																						
[COM_LAN]	Red Local																					
AMENAZAS	RIESGO POTENCIAL					CONTROLES/ SALVAGUARDAS EXISTENTES	NIVEL DE MADUREZ - CONTROLES EXISTENTES		RIESGO ACTUAL					CONTROLES/ SALVAGUARDAS SELECCIONADOS			NIVEL DE MADUREZ - CONTROLES ESTABLECIDOS		RIESGO PLANIFICADO				
	RIESGO POTENCIAL DIMENSIONES			RIESGO POTENCIAL TOTAL					RIESGO POR DIMENSIONES			RIESGO ACTUAL TOTAL							RIESGO POR DIMENSIONES			RIESGO TOTAL	
	Ri	Rc	Rd	Rt	NIVEL		NIVEL	PUNTOS	Ri	Rc	Rd	Rt	NIVEL			NIVEL	PUNTOS	Ri	Rc	Rd	Rt	NIVEL
5.2.9. [I.8] Fallo de servicios de comunicaciones	4	5	5	5	MUY ALTO	Existen controles para la gestión de acceso, donde únicamente el administrador tiene acceso a toda la red de la empresa. Existen controles referentes al uso aceptable de los activos relacionados a la red local. No existe un procedimiento que permita la separación de redes según las diferentes áreas de la empresa. Existe un procedimiento de control de acceso a la red, mediante el uso de contraseñas. Existe un control que permite la respuesta a incidentes de seguridad, en el caso de daños en la red local.	L1	1	3	4	4	4	ALTO	5.1.1	Políticas para la seguridad de la información.	L2	2	1	2	2	2	BAJO
5.3.2. [E.2] Errores del administrador	4	4	4	4	ALTO		L1	1	3	3	3	3	MODERADO	6.1.1	Roles y responsabilidades de seguridad de la información.	L2	2	1	1	1	1	MUY BAJO
5.3.11. [E.18] Destrucción de información	2	2	2	2	BAJO		L1	1	1	1	1	1	MUY BAJO	8.1.3	Uso aceptable de los activos.	L2	2	1	1	1	1	MUY BAJO
5.3.12. [E.19] Fugas de información	2	2	2	2	BAJO		L0	0	2	2	2	2	BAJO	9.1.1	Política de control de accesos.	L1	1	1	1	1	1	MUY BAJO
5.4.3. [A.5] Suplantación de la identidad del usuario	2	3	2	3	MODERADO		L1	1	1	2	1	2	BAJO	9.1.2	Control de acceso a las redes y servicios asociados.	L2	2	1	1	1	1	MUY BAJO
5.4.4. [A.6] Abuso de privilegios de acceso	3	3	3	3	MODERADO		L1	1	2	2	2	2	BAJO	12.4.1	Registro de eventos.	L2	2	1	1	1	1	MUY BAJO
5.4.9. [A.11] Acceso no autorizado	3	4	4	4	ALTO		L1	1	2	3	3	3	MODERADO	13.1.1	Controles de red.	L2	2	1	1	1	1	MUY BAJO
5.4.10. [A.12] Análisis de tráfico	4	4	4	4	ALTO		L1	1	3	3	3	3	MODERADO	13.1.3	Separación en las redes.	L2	2	1	1	1	1	MUY BAJO
5.4.13. [A.15] Modificación deliberada de la información	3	3	3	3	MODERADO		L1	1	2	2	2	2	BAJO	16.1.5	Respuesta a incidentes de seguridad de la información.	L2	2	1	1	1	1	MUY BAJO
5.4.15. [A.19] Divulgación de información	2	3	2	3	MODERADO		L0	0	2	3	2	3	MODERADO	17.1.1	Planificación de la continuidad de la seguridad de la información.	L1	1	1	2	1	2	BAJO
5.4.18. [A.24] Denegación de servicio	2	3	3	3	MODERADO		L1	1	1	2	2	2	BAJO			L2	2	1	1	1	1	MUY BAJO

- **REDES DE COMUNICACIONES: [COM_MB]**

Tabla I.38. Matriz de Gestión de Riesgos Actual y Planificado: [COM_MB]

[COM] REDES DE COMUNICACIONES																							
[COM_MB]	Telefonía Móvil																						
AMENAZAS	RIESGO POTENCIAL					CONTROLES/ SALVAGUARDAS EXISTENTES	NIVEL DE MADUREZ - CONTROLES EXISTENTES		RIESGO ACTUAL					CONTROLES/ SALVAGUARDAS SELECCIONADOS			NIVEL DE MADUREZ - CONTROLES ESTABLECIDOS		RIESGO PLANIFICADO				
	RIESGO POTENCIAL DIMENSIONES			RIESGO POTENCIAL TOTAL					RIESGO POR DIMENSIONES			RIESGO ACTUAL TOTAL							RIESGO POR DIMENSIONES			RIESGO TOTAL	
	Ri	Rc	Rd	Rt	NIVEL		NIVEL	PUNTOS	Ri	Rc	Rd	Rt	NIVEL				NIVEL	PUNTOS	Ri	Rc	Rd	Rt	NIVEL
5.2.9. [I.8] Fallo de servicios de comunicaciones	2	5	5	4	ALTO	Existe un control que permite el contacto directo con grupos de interés especial en el tema.	L1	1	1	4	4	3	MODERADO	5.1.1	Políticas para la seguridad de la información.		L2	2	1	2	2	2	BAJO
5.3.2. [E.2] Errores del administrador	2	4	4	4	ALTO		L1	1	1	3	3	3	MODERADO	6.1.1	Roles y responsabilidades de seguridad de la información.		L2	2	1	1	1	1	MUY BAJO
5.3.11. [E.18] Destrucción de información	2	3	3	3	MODERADO		L1	1	1	2	2	2	BAJO	8.1.3	Uso aceptable de los activos.		L2	2	1	1	1	1	MUY BAJO
5.3.12. [E.19] Fugas de información	5	5	5	5	MUY ALTO	No existe un backup de este servicio.	L0	0	5	5	5	5	MUY ALTO	9.1.1	Política de control de accesos.		L2	2	3	3	3	3	MODERADO
5.4.3. [A.5] Suplantación de la identidad del usuario	1	2	2	2	BAJO		L1	1	1	1	1	1	MUY BAJO	9.1.2	Control de acceso a las redes y servicios asociados.		L2	2	1	1	1	1	MUY BAJO
5.4.4. [A.6] Abuso de privilegios de acceso	2	3	3	3	MODERADO		L1	1	1	2	2	2	BAJO	12.4.1	Registro de eventos.		L2	2	1	1	1	1	MUY BAJO
5.4.9. [A.11] Acceso no autorizado	2	5	4	4	ALTO	Existe un procedimiento a seguir en el caso de fallos del servicio.	L1	1	1	4	3	3	MODERADO	13.1.1	Controles de red.		L2	2	1	2	1	2	BAJO
5.4.10. [A.12] Análisis de tráfico	1	2	2	2	BAJO		L0	0	1	2	2	2	BAJO	13.2.2	Acuerdos de transferencia de información.		L1	1	1	1	1	1	MUY BAJO
5.4.13. [A.15] Modificación deliberada de la información	2	2	2	2	BAJO		L1	1	1	1	1	1	MUY BAJO	16.1.5	Respuesta a incidentes de seguridad de la información.		L2	2	1	1	1	1	MUY BAJO
5.4.15. [A.19] Divulgación de información	5	5	3	5	MUY ALTO	No existe planificación de continuidad de seguridad de la información	L0	0	5	5	3	5	MUY ALTO	17.1.1	Planificación de la continuidad de la seguridad de la información.		L2	2	3	3	1	3	MODERADO
5.4.18. [A.24] Denegación de servicio	2	3	3	3	MODERADO		L1	1	1	2	2	2	BAJO				L2	2	1	1	1	1	MUY BAJO

- **REDES DE COMUNICACIONES: [COM_WF]**

Tabla I.39. Matriz de Gestión de Riesgos Actual y Planificado: [COM_WF]

[COM] REDES DE COMUNICACIONES																									
[COM_WF]	Red Inalámbrica																								
AMENAZAS	RIESGO POTENCIAL					CONTROLES/ SALVAGUARDAS EXISTENTES	NIVEL DE MADUREZ - CONTROLES EXISTENTES		RIESGO ACTUAL					CONTROLES/ SALVAGUARDAS SELECCIONADOS			NIVEL DE MADUREZ - CONTROLES ESTABLECIDOS		RIESGO PLANIFICADO					
	RIESGO POTENCIAL DIMENSIONES			RIESGO POTENCIAL TOTAL					RIESGO POR DIMENSIONES			RIESGO ACTUAL TOTAL							RIESGO POR DIMENSIONES			RIESGO TOTAL	
	Ri	Rc	Rd	Rt	NIVEL		NIVEL	PUNTOS	Ri	Rc	Rd	Rt	NIVEL			NIVEL	PUNTOS	Ri	Rc	Rd	Rt	NIVEL
5.2.9. [I.8] Fallo de servicios de comunicaciones	2	4	4	4	ALTO	Existen controles para la gestión de acceso, donde únicamente el administrador puede realizar cambios en las configuraciones de la red inalámbrica.	L1	1	1	3	3	3	MODERADO	5.1.1	Políticas para la seguridad de la información.	L2	2	1	1	1	1	MUY BAJO
5.3.2. [E.2] Errores del administrador	2	4	4	4	ALTO		L1	1	1	3	3	3	MODERADO	6.1.1	Roles y responsabilidades de seguridad de la información.	L2	2	1	1	1	1	MUY BAJO
5.3.11. [E.18] Destrucción de información	1	1	3	2	BAJO		L1	1	1	1	2	2	BAJO	8.1.3	Uso aceptable de los activos.	L2	2	1	1	1	1	MUY BAJO
5.3.12. [E.19] Fugas de información	4	4	3	4	ALTO	Existe un procedimiento de control de acceso a la red, mediante el uso de contraseñas.	L0	0	4	4	3	4	ALTO	9.1.1	Política de control de accesos.	L1	1	3	3	2	2	BAJO
5.4.3. [A.5] Suplantación de la identidad del usuario	2	3	2	3	MODERADO		L1	1	1	2	1	2	BAJO	9.1.2	Control de acceso a las redes y servicios asociados.	L2	2	1	1	1	1	MUY BAJO
5.4.4. [A.6] Abuso de privilegios de acceso	2	3	2	3	MODERADO	No existe un control que permita el análisis de tráfico y un registro de eventos aceptable.	L0	0	2	3	2	3	MODERADO	12.4.1	Registro de eventos.	L1	1	1	2	1	2	BAJO
5.4.9. [A.11] Acceso no autorizado	3	4	4	4	ALTO		L1	1	2	3	3	3	MODERADO	13.1.1	Controles de red.	L2	2	1	1	1	1	MUY BAJO
5.4.10. [A.12] Análisis de tráfico	2	2	2	2	BAJO	No existe planificación de continuidad de seguridad de la información	L0	0	2	2	2	2	BAJO	16.1.5	Respuesta a incidentes de seguridad de la información.	L1	1	1	1	1	3	MODERADO
5.4.13. [A.15] Modificación deliberada de la información	2	2	1	2	BAJO		L1	1	1	1	1	1	MUY BAJO	17.1.1	Planificación de la continuidad de la seguridad de la información.	L2	2	1	1	1	1	MUY BAJO
5.4.15. [A.19] Divulgación de información	4	4	3	4	ALTO		L1	1	3	3	2	3	MODERADO			L1	1	2	2	1	2	BAJO
5.4.18. [A.24] Denegación de servicio	2	3	3	3	MODERADO		L1	1	1	2	2	2	BAJO			L2	2	1	1	1	1	MUY BAJO

- **EQUIPO AUXILIAR: [AUX_CB]**

Tabla I.40. Matriz de Gestión de Riesgos Actual y Planificado: [AUX_CB]

[AUX] EQUIPO AUXILIAR																									
[AUX_CB]	Cableado Estructurado																								
AMENAZAS	RIESGO POTENCIAL					CONTROLES/ SALVAGUARDAS EXISTENTES	NIVEL DE MADUREZ - CONTROLES EXISTENTES		RIESGO ACTUAL					CONTROLES/ SALVAGUARDAS SELECCIONADOS			NIVEL DE MADUREZ - CONTROLES ESTABLECIDOS		RIESGO PLANIFICADO					
	RIESGO POTENCIAL DIMENSIONES			RIESGO POTENCIAL TOTAL					RIESGO POR DIMENSIONES			RIESGO ACTUAL TOTAL							RIESGO POR DIMENSIONES				RIESGO TOTAL	
	Ri	Rc	Rd	Rt	NIVEL		NIVEL	PUNTOS	Ri	Rc	Rd	Rt	NIVEL				NIVEL	PUNTOS	Ri	Rc	Rd	Rt	NIVEL	
5.1.1. [N.1] Fuego	1	1	2	2	BAJO	Existen controles para la gestión de activos y la restauración de estos.	L1	1	1	1	1	1	MUY BAJO	5.1.1	Políticas para la seguridad de la información.		L2	2	1	1	1	1	MUY BAJO	
5.1.2. [N.2] Daños por agua	2	3	4	3	MODERADO		L1	1	1	2	3	2	BAJO	6.1.1	Roles y responsabilidades de seguridad de la información.		L2	2	1	1	1	1	MUY BAJO	
5.2.3. [I.*] Desastres industriales	1	1	2	2	BAJO		L1	1	1	1	1	1	MUY BAJO	8.1.1	Inventario de activos.		L2	2	1	1	1	1	MUY BAJO	
5.2.4. [I.3] Contaminación mecánica	2	2	4	3	MODERADO	Existen controles referentes al uso aceptable de los activos relacionados al cableado estructurado.	L0	0	2	2	4	3	MODERADO	8.1.3	Uso aceptable de los activos.		L1	1	1	1	3	2	BAJO	
5.2.6. [I.5] Avería de origen físico o lógico	2	2	3	3	MODERADO		L1	1	1	1	2	2	BAJO	9.1.1	Política de control de accesos.		L2	2	1	1	1	1	MUY BAJO	
5.2.7. [I.6] Corte del suministro eléctrico	3	2	5	4	ALTO		L0	0	3	2	5	4	ALTO	9.1.2	Control de acceso a las redes y servicios asociados.		L1	1	2	1	4	3	MODERADO	
5.2.10. [I.9] Interrupción de otros servicios y suministros esenciales	2	3	5	4	ALTO	Existe un control que permite la respuesta a incidentes de seguridad, en el caso de daños en la red local.	L1	1	1	2	4	3	MODERADO	12.4.1	Registro de eventos.		L2	2	1	1	1	1	MUY BAJO	
5.3.15. [E.23] Errores de mantenimiento / actualización de equipos (hardware)	3	3	3	3	MODERADO		L0	0	3	3	3	3	MODERADO	13.1.1	Controles de red.		L1	1	2	2	2	2	BAJO	
5.3.17. [E.25] Pérdida de equipos	3	4	4	4	ALTO	No existe un control que especifique el etiquetado de los equipos de hardware y cableado estructurado.	L1	1	2	3	3	3	MODERADO	16.1.5	Respuesta a incidentes de seguridad de la información.		L2	2	1	1	1	1	MUY BAJO	
5.4.9. [A.11] Acceso no autorizado	2	4	3	3	MODERADO		L1	1	1	3	2	2	BAJO	17.1.1	Planificación de la continuidad de la seguridad de la información.		L2	2	1	1	1	1	MUY BAJO	
5.4.17. [A.23] Manipulación de los equipos	4	4	4	4	ALTO	Existe un control que permite la respuesta a incidentes de seguridad, en el caso de daños en la red local.	L0	0	4	4	4	4	ALTO				L1	1	3	3	3	3	MODERADO	
5.4.19. [A.25] Robo	2	2	2	2	BAJO		L1	1	1	1	1	1	MUY BAJO				L2	2	1	1	1	1	MUY BAJO	

- **EQUIPO AUXILIAR: [AUX_VIDEO]**

Tabla I.41. Matriz de Gestión de Riesgos Actual y Planificado: [AUX_VIDEO]

[AUX] EQUIPO AUXILIAR																									
[AUX_VIDEO]	Sistema de Video vigilancia																								
AMENAZAS	RIESGO POTENCIAL					CONTROLES/ SALVAGUARDAS EXISTENTES	NIVEL DE MADUREZ - CONTROLES EXISTENTES		RIESGO ACTUAL					CONTROLES/ SALVAGUARDAS SELECCIONADOS		NIVEL DE MADUREZ - CONTROLES ESTABLECIDOS		RIESGO PLANIFICADO					
	RIESGO POTENCIAL DIMENSIONES			RIESGO POTENCIAL TOTAL					RIESGO POR DIMENSIONES			RIESGO ACTUAL TOTAL							RIESGO POR DIMENSIONES			RIESGO TOTAL	
	Ri	Rc	Rd	Rt	NIVEL		NIVEL	PUNTOS	Ri	Rc	Rd	Rt	NIVEL			NIVEL	PUNTOS	Ri	Rc	Rd	Rt	NIVEL		
5.1.1. [N.1] Fuego	1	1	2	2	BAJO	Existen controles para la gestión de acceso, donde únicamente el administrador tiene acceso al equipo.	L1	1	1	1	1	1	MUY BAJO	5.1.1	Políticas para la seguridad de la información.	L2	2	1	1	1	1	MUY BAJO	
5.1.2. [N.2] Daños por agua	2	3	4	3	MODERADO		L1	1	1	2	3	2	BAJO	6.1.1	Roles y responsabilidades de seguridad de la información.	L2	2	1	1	1	1	MUY BAJO	
5.2.3. [I.*] Desastres industriales	1	1	2	2	BAJO		L1	1	1	1	1	1	MUY BAJO	8.1.1	Inventario de activos.	L2	2	1	1	1	1	MUY BAJO	
5.2.4. [I.3] Contaminación mecánica	2	2	4	3	MODERADO		L0	0	2	2	4	3	MODERADO	8.1.3	Uso aceptable de los activos.	L1	1	1	1	2	2	BAJO	
5.2.6. [I.5] Avería de origen físico o lógico	2	2	3	3	MODERADO	Existen controles referentes a las configuraciones de los equipos de red.	L1	1	1	1	2	2	BAJO	9.1.1	Política de control de accesos.	L2	2	1	1	1	1	MUY BAJO	
5.2.7. [I.6] Corte del suministro eléctrico	4	4	4	4	ALTO		L0	0	4	4	4	4	ALTO	9.1.2	Control de acceso a las redes y servicios asociados.	L1	1	2	2	2	2	BAJO	
5.2.10. [I.9] Interrupción de otros servicios y suministros esenciales	3	3	4	4	ALTO		L1	1	2	2	3	3	MODERADO	12.4.1	Registro de eventos.	L2	2	1	1	1	1	MUY BAJO	
5.3.15. [E.23] Errores de mantenimiento / actualización de equipos (hardware)	2	3	3	3	MODERADO	Existe un procedimiento de control de acceso al sistema de video vigilancia, mediante el uso de contraseñas.	L0	0	2	3	3	3	MODERADO	12.5.1	Instalación del software en los sistemas operativos.	L1	1	1	2	2	2	BAJO	
5.3.17. [E.25] Pérdida de equipos	1	3	4	3	MODERADO		L1	1	1	2	3	2	BAJO	13.1.1	Controles de red.	L2	2	1	1	1	1	MUY BAJO	
5.4.9. [A.11] Acceso no autorizado	2	4	4	4	ALTO		L1	1	1	3	3	3	MODERADO	16.1.5	Respuesta a incidentes de seguridad de la información.	L2	2	1	1	1	1	MUY BAJO	
5.4.17. [A.23] Manipulación de los equipos	3	3	3	3	MODERADO	No existe planificación de continuidad de seguridad de la información	L0	0	3	3	3	3	MODERADO	17.1.1	Planificación de la continuidad de la seguridad de la información.	L1	1	2	2	2	2	BAJO	
5.4.19. [A.25] Robo	1	2	2	2	BAJO		L1	1	1	1	1	1	MUY BAJO			L2	2	1	1	1	1	MUY BAJO	

- **EQUIPO AUXILIAR: [AUX_UPS]**

Tabla I.42. Matriz de Gestión de Riesgos Actual y Planificado: [AUX_UPS]

[AUX] EQUIPO AUXILIAR																									
[AUX_UPS]	Sistema de alimentación Interrumpida																								
AMENAZAS	RIESGO POTENCIAL					CONTROLES/ SALVAGUARDAS EXISTENTES	NIVEL DE MADUREZ - CONTROLES EXISTENTES		RIESGO ACTUAL					CONTROLES/ SALVAGUARDAS SELECCIONADOS		NIVEL DE MADUREZ - CONTROLES ESTABLECIDOS		RIESGO PLANIFICADO				
	RIESGO POTENCIAL POR DIMENSIONES			RIESGO POTENCIAL TOTAL					RIESGO POR DIMENSIONES			RIESGO ACTUAL TOTAL						RIESGO POR DIMENSIONES			RIESGO TOTAL	
	Ri	Rc	Rd	Rt	NIVEL		NIVEL	PUNTOS	Ri	Rc	Rd	Rt	NIVEL			NIVEL	PUNTOS	Ri	Rc	Rd	Rt	NIVEL
5.1.1. [N.1] Fuego	1	1	2	2	BAJO	No existen políticas referentes al inventario de activos. Existe un control que indica el uso adecuado del activo evaluado. No existe planificación de continuidad de seguridad de la información	L1	1	1	1	1	1	MUY BAJO	5.1.1	Políticas para la seguridad de la información.	L2	2	1	1	1	1	MUY BAJO
5.1.2. [N.2] Daños por agua	1	2	2	2	BAJO		L1	1	1	1	1	1	MUY BAJO	8.1.1	Inventario de activos.	L2	2	1	1	1	1	MUY BAJO
5.2.3. [I.*] Desastres industriales	1	1	2	2	BAJO		L1	1	1	1	1	1	MUY BAJO	8.1.3	Uso aceptable de los activos.	L2	2	1	1	1	1	MUY BAJO
5.2.4. [I.3] Contaminación mecánica	2	2	2	2	BAJO		L0	0	2	2	2	2	BAJO	16.1.5	Respuesta a incidentes de seguridad de la información.	L1	1	1	1	1	1	MUY BAJO
5.2.6. [I.5] Avería de origen físico o lógico	2	2	2	2	BAJO		L1	1	1	1	1	1	MUY BAJO	17.1.1	Planificación de la continuidad de la seguridad de la información.	L2	2	1	1	1	1	MUY BAJO
5.2.7. [I.6] Corte del suministro eléctrico	3	3	3	3	MODERADO		L0	0	3	3	3	3	MODERADO			L1	1	2	2	2	2	BAJO
5.3.15. [E.23] Errores de mantenimiento / actualización de equipos (hardware)	1	2	2	2	BAJO		L1	1	1	1	1	1	MUY BAJO			L2	2	1	1	1	1	MUY BAJO
5.3.17. [E.25] Pérdida de equipos	2	2	2	2	BAJO		L1	1	1	1	1	1	MUY BAJO			L2	2	1	1	1	1	MUY BAJO
5.4.17. [A.23] Manipulación de los equipos	2	1	2	2	BAJO		L0	0	2	1	2	2	BAJO			L1	1	1	1	1	1	MUY BAJO
5.4.19. [A.25] Robo	1	1	1	1	MUY BAJO		L1	1	1	1	1	1	MUY BAJO			L2	2	1	1	1	1	MUY BAJO

ORDEN DE EMPASTADO